MANAJEMEN RISIKO IT PADA SISTEM IRAISE MENGGUNAKAN METODE NIST SP 800-30

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

YUSRIKA DEWI
11353204459

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2021

LEMBAR PERSETUJUAN

MANAJEMEN RISIKO IT PADA SISTEM IRAISE MENGGUNAKAN METODE NIST SP 800-30

TUGAS AKHIR

Oleh:

YUSRIKA DEWI
11353204459

Telah diperiksa dan disetujui sebagai laporan tugas akhir
di Pekanbaru, pada tanggal 19 Februari 2021

Ketua Program Studi	Pembimbing
Idria Maita, S.Kom., M.Sc.	M. Afdal, ST., M.Kom.
NIP. 19790513200710200 5	NIK. 130517052

LEMBAR PENGESAHAN

MANAJEMEN RISIKO IT PADA SISTEM IRAISE MENGGUNAKAN METODE NIST SP 800-30

TUGAS AKHIR

Oleh:

YUSRIKA DEWI
11353204459

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 09 Februari 2021

Pekanbaru, 09 Februari 2021
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Drs. Ahmad Darmawi, M.Ag.	Idria Maita, S.Kom., M.Sc.
NIP. 196606041992031004	NIP. 197905132007102005

DEWAN PENGUJI:

Ketua : **Arif Marsal, Lc., MA.**

Sekretaris : **M. Afdal, ST., M.Kom.**

Anggota 1 : **Eki Saputra, S.Kom., M.Kom.**

Anggota 2 : **Nesdi Evrilyan Rozanda, S.Kom. M.Sc.**

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin penulis dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan didalam daftar pustaka.

Pekanbaru, 09 Februari 2021
Yang membuat pernyataan,

YUSRIKA DEWI
NIM. 11353204459

LEMBAR PERSEMBAHAN

Tugas akhir ini saya persembahkan untuk kedua orang tua saya, Ayah dan mamak, Kakak dan adik-adik. Terima kasih untuk segala hal baik yang kalian berikan, semangat, kasih sayang yang tulus, serta do'a yang tidak pernah putus.

Tak lupa pula saya mengucapkan terimakasih kepada Bapak dan Ibu Dosen, Pembimbing dan penguji tugas akhir yang dengan ikhlas memberikan ilmu, pengetahuan, dan pembelajaran berharga selama masa perkuliahan. Semoga Allah SWT membalas jasa-jasa kalian.

Untuk teman-teman SIF 2013 dan keluarga besar PTIPD UIN SUSKA Riau, teman-teman kos Ar-rahmah. Terimakasih atas dukungan, bantuan dan motivasi kalian sehingga saya dapat melewati ini semua. Untuk diriku sendiri yang berhasil melewati segala proses perkuliahan hingga menyelesaikan tugas akhir ini.

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh.

Alhamdulillahirabbil 'alamiin, puji syukur diucapkan kepada Allah SWT yang telah melimpahkan rahmat, nikmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul **"Manajemen Risiko IT Pada Sistem Iraise Menggunakan Metode NIST SP 800-300"** yang merupakan sebagai salah satu syarat untuk mencapai gelar kesarjanaan pada Program Studi Sistem Informasi Universitas Islam Negeri Sultan Syarif Kasim Riau. Shalawat serta salam selalu tercurahkan kepada junjungan Nabi Muhammad SAW dengan ucapan "Allahumma sholli 'ala Muhammad wa'ala ali Muhammad" yang telah menjadi suri tauladan yang baik bagi kita semua.

Dalam penyusunan Tugas Akhir ini, penulis menyadari bahwa hal yang dilakukan penulis pada penyusunan laporan Tugas Akhir ini masih jauh dari kata sempurna. Oleh karena itu, penulis sangat mengharapkan kritik disertai dengan saran yang membangun dan berguna dalam penyusunan Tugas Akhir ini dimasa yang akan datang, semoga hal yang telah penulis lakukan ini dapat bermanfaat bagi pembaca.

Penulis juga mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam penyelesaian Tugas Akhir ini, baik secara langsung atau tidak langsung. Ucapan terima kasih penulis sampaikan kepada:

1. Bapak Prof. Dr. Suyitno, M.Ag., Plt Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Bapak Dr. Drs. Ahmad Darmawi, M.Ag., Dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau.
3. Ibu Idria Maita, S.Kom., M.Sc., Ketua Program Studi Sistem Informasi.
4. Bapak Eki Saputra, S.Kom., M.Kom., Sekretaris dan Penguji satu Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
5. Bapak Arif Marsal, Lc., MA., Ketua Sidang Tugas Akhir yang telah meluangkan waktunya dan memberikan masukan berupa kritik dan saran untuk Tugas Akhir ini.
6. Bapak M. Afdal, ST., M.Kom., dosen pembimbing tugas akhir ini, yang telah membimbing tugas akhir ini sampai selesai dan memberikan ilmu-ilmu pengetahuan yang baru bagi saya.
7. Bapak Nesdi Evrilyan Rozanda, S.Kom. M.Sc., penguji dua, yang juga banyak memberikan kritikan, arahan, serta saran yang membangun dalam

penyelesaian Tugas Akhir ini.

8. Mustaqim, ST., M.Kom., dosen Pembimbing Akademik selama perkuliahan yang selalu memberikan semangat, nasehat, arahan, saran serta membimbing yang sangat baik.
9. Segenap Dosen dan Karyawan Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau, terima kasih atas ilmu yang telah diberikan.
10. Keluargaku tercinta Ayah dan Mamak sebagai motivator utama dalam penyelesaian Tugas Akhir ini karena telah memberikan dukungan moril maupun materil, do'a, perhatian, kasih sayang, dan semangat tiada henti. Kakak dan adek-adek ku yang memberi do'a, semangat, dan dukungan hingga selesainya Tugas Akhir ini.
11. Terimakasih untuk sahabat-sahabat ku, Ade Irmayani, Ninuk Desfitri, Nurul Hidayanti, Kak Azmi Ila Adini, Melly Angraini, Rosalina Sari, Annisa Utamy, Muhammad Hargono, Dwi Widiastuti, Boby Rahman dan Sistem Informasi A angkatan 2013, keluarga besar PTIPD UIN Suska Riau dan yang tidak bisa saya sebutkan satu-persatu, yang memberikan inspirasi, semangat, dan membantu penulis dari awal sampai selesai penulisan Tugas Akhir ini.

Penulis menyadari dalam penulisan laporan ini masih banyak kesalahan dan kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk kesempurnaan laporan ini dan dapat disampaikan ke email yusrika.dewi@students.ac.id sehingga lebih baik dan bermanfaat bagi yang membutuhkannya.

Pekanbaru, 19 Februari 2021

Penulis,

YUSRIKA DEWI

NIM. 11353204459

MANAJEMEN RISIKO IT PADA SISTEM IRAISE MENGGUNAKAN METODE NIST SP 800-30

YUSRIKA DEWI
NIM: 11353204459

Tanggal Sidang: 09 Februari 2021
Periode Wisuda:

Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. Soebrantas, No. 155, Pekanbaru

ABSTRAK

Universitas Islam Negeri Sultan Syarif Kasim Riau (UIN SUSKA RIAU) merupakan universitas yang menggunakan teknologi informasi sebagai pendukung proses akademik. Sistem informasi yang diberi nama *Intregated Academic Information System* (iRaise) merupakan salah satu teknologi informasi yang digunakan UIN Suska Riau. Terkait dengan penerapan Sistem Informasi dan teknologi tidak lepas dari adanya ancaman yang berpotensi mengganggu proses akademik. Untuk mencegah kerugian akibat adanya potensi bahaya maka diperlukan suatu perhitungan risiko. Tujuan Penelitian ini untuk mengidentifikasi dan meminimalisir risiko yang akan terjadi pada penggunaan system iRaise. Penelitian ini menggunakan metode NIST SP 800-30 dan 9 Langkah didalamnya yaitu mengenali karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, analisis pengendalian, penentuan kemungkinan, analisis dampak, penentuan risiko, rekomendasi pengendalian, dan dokumentasi hasil. Pada proses pengolahan data dihasilkan ancaman-ancaman yang sudah teridentifikasi yaitu kebakaran, *human error*, *virus*, *hacking* dan kegagalan jaringan. Pada proses identifikasi ancaman ditemukan tingkat risiko yang berbeda pada tiap kategori *level* risiko. Hasil akhir penelitian ini berupa rekomendasi kontrol yang disarankan terhadap ancaman risiko yang terjadi, sehingga dapat menjadi acuan bagi instansi untuk dapat digunakan untuk *control* selanjutnya.

Kata Kunci: iRaise, Manajemen Risiko, NIST, PTIPD, UIN SUSKA RIAU

IT RISK MANAGEMENT ON IRAISE SYSTEM USING THE NIST SP 800-30 METHODE

YUSRIKA DEWI
NIM: 11353204459

Date of Final Exam: February 09th 2021
Graduation Period:

Department of Information System
Faculty of Science and Technology
State Islamic University of Sultan Syarif Kasim Riau
Soebrantas Street, No. 155, Pekanbaru

ABSTRACT

State Islamic University Of Sultan Syarif Kasim Riau (UIN SUSKA RIAU) is a university that uses information technology to support the academic process. The information system called the Integrated Academic Information System (iRaise) is one of the information technologies used by UIN Suska Riau. Regarding the application of Information Systems and the use of technology, some threats have the potential to disrupt the academic process. To prevent losses due to potential hazards, a risk calculation is required. The purpose of this study is to identify and minimize the risks that will occur in using the IRAISE system. This study uses the NIST SP 800-30 method and the 9 steps in it, namely recognizing system characteristics, identifying threats, identifying vulnerabilities, controlling analysis, determining likelihood, impact analysis, determining risk, controlling recommendations, and documenting results. In the data processing process, identified threats are generated, namely fire, human error, viruses, hacking and network failure. In the process of identifying threats, a different level of risk is found for each category of the risk level. The final result of this research is in the form of recommended control recommendations against the risks that occur so that it can become a reference for agencies to be used for further control.

Keywords: *iRaise, NIST, Risk Management, PTIPD and UIN Suska RIAU*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

BCP	:	*Business Continuity Plan*
ERP	:	*Enterprise Resource Planning*
FO	:	*Fiber Optic*
IT	:	*Information technology*
ISP	:	*Internet Service Provider*
iRaise	:	*Intregated Academic Information System*
KHS	:	Kartu Hasil Studi
KRS	:	Kartu Rencana Studi
NIST	:	*National Institute of Standard and Technology*
POK	:	Pedoman Operasional Kegiatan
PUSKOM	:	Pusat Komputer
PTIPD	:	Pusat Teknologi Informasi dan Pangkalan Data
RPO	:	*Recovery Point Objectives*
RIPTI	:	Rencana Induk Pengembangan Teknologi Informasi
RTO	:	*Recovery Time Objectives*
SIMAK	:	Sistem Informasi Akademik
SDLC	:	*Software Development Life Cycle*
SP	:	*Special Publication*
SOP	:	Standard Operating Prosedur
UPS	:	*Uninterruptible Power Supply*
UPT	:	Unit Pelaksana Teknis
UIN	:	Universitas Islam Negeri

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Manajemen risiko adalah suatu proses identifikasi, mengatur risiko, serta membentuk strategi untuk mengelola risiko melalui sumber daya yang tersedia. Strategi yang dapat digunakan yaitu dengan cara penanganan risiko yang akan terjadi, meminimalisir risiko, menghindari kemungkinan risiko, dan mengurangi efek buruk dari risiko. Usaha-usaha untuk meminimalisir risiko ataupun mengatasi risiko-risiko yang telah terjadi didalam proses bisnis dapat dilakukan dengan manajemen risiko (Viyanto, Latuihamallo, Tua, Gui, dan Suryanto, 2013).

Penelitian yang dilakukan oleh Febriyanti dan Hidayanto (2012), yang membahas tentang pengelolaan data TI yang berbasis risiko pada PT. Petrokimia Gresik. Metode yang digunakan dalam mengelola risiko adalah NIST SP 800-30 yang dimulai dari mengidentifikasi risiko, menilai risiko serta membentuk strategi untuk mengelolanya. Maka didapat beberapa masalah pada saat proses pengelolahan data dihasilkan risiko-risiko yang sudah teridentifikasi dan risiko yang ada dalam proses pengelolaan keamanan sistem informasi seperti kebakaran, *virus*, *human error*, *hacking*, kehilangan data yang tidak berhasil di backup dan restore.

Universitas Islam Negeri Sultan Syarif Kasim Riau (UIN SUSKA RIAU) merupakan salah satu universitas yang menggunakan teknologi informasi sebagai pendukung visi dan misi menjadi *world class university*. Teknologi informasi diterapkan dengan menggunakan suatu sistem informasi yang dapat mempermudah proses-proses yang berkaitan dengan akademik serta menjadi sarana komunikasi antar civitas Akademik. Sistem Akademik yang diberi nama *Intregated Academic Information System* atau lebih dikenal dengan sebutan iRaise adalah sistem generasi ketiga UIN Suska Riau. Sistem ini diluncurkan sebagai pengganti Sistem Informasi Akademik (SIMAK) yang lama. Pengembangan Sistem Informasi Akademik Terpadu (iRaise) menjadi mendesak, karena jumlah mahasiswa UIN Suska Riau yang semakin meningkat hingga mencapai 30 ribu mahasiswa, sehingga tidak memungkinkan lagi untuk dilakukan layanan secara manual mengingat pula jumlah pegawai dan sumber daya manusia yang terbatas. Karena itu diperlukan adanya Sistem layanan Informasi dan Akademik yang lebih efektif dan efisien.

Dengan adanya penggunaan yang tinggi terhadap Sistem iRaise maka harus dimbangi dengan pengaturan dan pengelolaan risiko yang tepat agar kemungkinan terjadinya risiko dapat dihindari sehingga tidak menyebabkan kerugian dan pengambilan keputusan yang salah. Terkait dengan penerapan Sistem Informasi dan

penggunaan teknologi tidak lepas dari adanya ancaman yang berpotensi menggang-gu keberlangsungan proses akademik. Ancaman tersebut berupa kehilangan data, kurangnya keamanan sistem, kerusakan akibat bencana alam ataupun kesalahan dari orang yang terlibat langsung dengan organisasi. Namun ancaman-ancaman terse-but dapat dihindari jika organisasi dapat merencanakan atau mengantisipasi langkah aman jika timbul kegagalan. Untuk mengetahui ancaman dan risiko keamanan yang mungkin terjadi dan dapat mempengaruhi proses akademik serta menimbulkan kerugian instansi, maka dari itu perlu diperlukan sebuah metode atau kerangka kerja untuk membantu proses penilaian risiko.

Berdasarkan hasil wawancara dengan kepala PTIPD dan kepala divisi sis-tem jaringan dan pangkalan data terdapat beberapa masalah pada iRaise yaitu per-nah mengalami serangan seperti *web deface*, sistem disisipi *shell*, pemalsuan a-plikasi dalam bentuk *mobile*, kabel *fiber optic* yang beberapa kali sempat putus saat kegiatan pembangunan dan perangkat disambar petir serta kapasitas server yang kurang memadai sehingga iRaise sering mengalami down saat diakses secara bersamaan.

Berdasarkan permasalahan diatas maka penulis melakukan penelitian un-tuk penilaian risiko terhadap sistem iRaise dengan menggunakan metode NIST SP 800-30. Sebenarnya ada beberapa metode yang dapat digunakan untuk melakukan manajemen risiko keamanan informasi seperti Octave, ISO 27001 dan NIST SP 800-30. Metode NIST SP 800-30 merupakan panduan manajemen risiko untuk sistem teknologi informasi yang merupakan standar pemerintah Amerika Serikat (Eiky, 2007). Metodologi ini dirancang menjadi suatu perhitungan kualitatif dan dilasarkan pada analisa keamanan yang cukup sesuai dengan keinginan pemilik sistem dalam mengevaluasi dan mengelola risiko dalam sistem TI. Proses ini sa-ngat komprehensif, meliputi segala sesuatu dari ancaman sumber identifikasi untuk evaluasi berkelanjutan dan penilaian. NIST (*National Institute of Standard and Technology*) mengeluarkan rekomendasi melalui publikasi khusus 800-30 tentang *Risk Management Guide for Information Technology System* dan merupakan metode terbaik dari 3 metode untuk analisa risiko yaitu Mehari, Magerit, dan *Microsoft's Security Management Guide* (Syalim, Hori, dan Sakurai, 2009).

Metode ini memiliki 9 Langkah yaitu mengenali karakteristik sistem, identi-fikasi ancaman, identifikasi kerentanan, analisis pengendalian, penentuan kemung-kinan, analisis dampak, penentuan risiko, rekomendasi pengendalian, dan doku-mentasi hasil.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan diatas, maka dapat dirumuskan permasalahan yaitu "Bagaimana manajemen risiko pada Sistem Informasi iRaise dalam Penggunaan Teknologi Informasi dan meminimalisir risiko-risiko yang akan terjadi menggunakan Metode NIST *Special Publication* 800-30?.

1.3 Batasan Masalah

Batasan masalah dalam penulisan tugas akhir ini adalah:

1. Penilaian risiko dilakukan pada bagian Divisi TI yang bertanggung jawab dan mengelola Sistem Informasi iaise.
2. Penelitian ini mengukur besarnya dampak risiko menggunakan metode NIST SP 800-30.
3. Pengumpulan dan analisis data menggunakan lembar kerja metode NIST SP 800-30.

1.4 Tujuan

Adapun tujuan yang ingin dicapai dari penelitian ini adalah:

1. Untuk melakukan identifikasi terhadap risiko-risiko atau ancaman yang akan terjadi pada sistem informasi iRaise.
2. Untuk melakukan pengukuran terhadap besarnya risiko-risiko yang telah diidentifikasi pada sistem informasi iRaise.
3. Untuk menentukan hasil penilaian risiko keamanan teknologi informasi.

1.5 Manfaat

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Hasil dari pengukuran dan analisa yang dilakukan dapat dijadikan informasi bagi PTIPD UIN Suska Riau.
2. Memeberikan rekomendasi atas penanganan risiko penerapan teknologi informasi sebagai solusi untuk dapat mendukung proses bisnis dan membantu dalam mengurangi kerugian.
3. Mengetahui seberapa besar tingkat risiko yang terjadi apada PTIPD UIN Suska Riau.

1.6 Sistematika Penulisan

Sistematika pembahasan laporan penelitian ini terdiri dari pokok-pokok permasalahan yang dibahas pada masing-masing bab, berikut merupakan sistematika pembahasan pada penelitian ini:

BAB 1. PENDAHULUAN

Bab 1 pada tugas akhir ini berisi tentang: (1) Latar Belakang; (2) Perumu-

san Masalah; (3) Batasan Masalah; (4) Tujuan; (5) Manfaat; dan (6) Sistematika Penulisan.

BAB 2. LANDASAN TEORI

Bab 2 pada tugas akhir ini berisi tentang: (1) Ruang Lingkup Manajemen; (2) Manajemen Risiko Teknologi Infomasi; (3) Keamanan Sistem Informasi; (4) Pengertian Ancaman, Kemungkinan dan Dampak; (5) Metode Pengukuran Risiko IT; (6) Profil Perusahaan; (7) Visi, Misi dan Tujuan PTIPD UIN Suska Riau; (8) Struktur Organisasi, Peranan dan Tugas Pokok PTIPD UIN Suska Riau; (9) iRaise; (10) Peneitian Terdahulu.

BAB 3. METODOLOGI PENELITIAN

Bab 3 pada tugas akhir ini berisi tentang: (1) Kerangka Peneitian; (2) Tahap Pengumpulan Data; (3) Tahap Pengumpulan Data; (4) Tahap Penilaian Risiko IT

BAB 4. ANALISA DAN HASIL

Bab 4 pada tugas akhir ini berisi tentang: (1) Karakteristik Sistem; (2) Identifikasi Ancaman; (3) Identifikasi Kerentanan; (4) Analisa Kontrol; (5) Penentuan Kemungkinan; (6) Analisa Dampak; (7) Penentuan Risiko; (8) Rekonmendasi Kontrol; (9) Dokumentasi.

BAB 5. KESIMPULAN

Bab 5 pada tugas akhir ini berisi tentang: (1) Kesimpulan; (2) Saran.

BAB 2
LANDASAN TEORI

2.1 Ruang Lingkup Manajemen Risiko

Manajemen risiko adalah identifikasi, penilaian, dan prioritas risiko yang diikuti oleh aplikasi terkoordinasi dan ekonomis dari sumber daya untuk meminimalkan, menghindari, memantau, dan mengendalikan probabilitas atau kemungkinan dampak peristiwa yang tidak diinginkan dan dapat merugikan (Hubbard, 2009).

2.1.1 Pengertian Risiko

Risiko merupakan suatu kejadian terhadap suatu hal yang tidak tercapai atau yang seharusnya tidak dilakukan (Gondodiyoto, 2007). Risiko pada umumnya dipandang sebagai sesuatu yang negatif, seperti kehilangan, bahaya, dan konsekuensi lainnya. Risiko juga didefenisikan sebagai peluang terjadinya sesuatu yang dapat memberikan dampak atau mengakibatkan terganggunya proses bisnis sampai menyebabkan gagalnya tujuan bisnis Organisasi. Kerugian tersebut sebenarnya merupakan bentuk ketidakpastian yang seharusnya dipahami dan dikelola secara efektif oleh organisasi sebagai bagian dari strategi sehingga dapat menjadi nilai tambah dan mendukung pencapaian tujuan organisasi.

2.1.2 Macam-macam Risiko

Menurut Gondodiyoto (2007), Risiko yang biasa terjadi dapat berupa ancaman terhadap keamanan yang disebabkan oleh faktor alam, manusia yang bersifat kelalaian atau kesengajaan, antara lain:

1. Ancaman kebakaran yang di sebabkan oleh alam atau manusia

   Beberapa pelaksanaan keamanan untuk ancaman kebakaran sebagai berikut:

   (a) Memiliki alat pemadam kebakaran otomatis dan tabung pemadam kebakaran.
   (b) Memiliki pintu atau tangga darurat.
   (c) Melakukan pengecekan rutin dan pengujian terhadap sistem perlindungan kebakaran untuk memastikan segala sesuatunya dirawat dengan baik.

2. Ancaman Banjir

   Beberapa pelaksanaan pengamanan untuk ancaman banjir sebagai berikut:

   (a) Bahan atap, dinding dan lantai yang tahan terhadap air.
   (b) Semua material aset informasi terletak di tempat yang tinggi.
   (c) Perubahan tegangan sumber energi.
   (d) Pelaksanaan pengaman untuk mengantisipasi perubahan tegangan

sumber energi, misalnya: menggunakan *Stabilizer* atau *Uninterruptible Power Supplay* (UPS).

3. Kerusakan Strukural

Pelaksanaan pengaman untuk antisipasi kerusakan struktural misalnya seperti:

(a) memilih lokasi perusahaan yang strategis

(b) lokasi yang jarang terjadi gempa, angin ribut, dan banjir.

4. Penyusup

Pelaksanaan pengamanan untuk mengantisipasi penyusup adalah menempatkan penjaga dan penggunaan alarm atau kamera pengawas.

5. *Virus*

Pelaksanaan pengamanan untuk mengantisipasi *virus* adalah:

(a) *Preventif*, seperti memasang anti *virus* dan melakukan *update* secara rutin.

(b) *Detektif*, misalnya melakukan *scan file* sebelum digunakan

(c) *Korektif*, misalnya memastikan *backup data* bebas *virus*, pemakaian anti *virus* terhadap *file* yang terinfeksi.

6. *Hacking*

Beberapa pelaksanaan pengamanan untuk mengantisipasi *hacking* sebagai beikiut:

(a) Penggunaan *control logical* seperti penggunaan *password* yang sulit ditebak oleh orang lain.

(b) Petugas keamanan secara teratur dan konsisten memonitor sistem yang digunakan.

7. Kegagalan jaringan, kegagalan sistem dan data Beberapa pelaksanaan pengamanan untuk mengantisipasi risiko tersebut adalah:

(a) *Recovery Time Objectives* (RTO) adalah lama waktu yang dibutuhkan untuk pemulihan sistem dan data. Jika antar komponen layanan atau *service component* terjadi *dependency*, maka waktu *recovery* dihitung secara serial untuk komponen-komponen yang *interdepencency*. Jika antar komponen layanan tidak saling bergantung, recovery time dapat dihitung secara paralel antara komponen layanan. Maksimum RTO adalah 80% dari maksimum waktu layanan tidak befungsi yang ditoleransi atau MTDL.

(b) *Recovery Point Objectives*(RPO) adalah ambang berapa banyak data yang boleh hilang sejak terakhir backup dilakukan. Jika *backup* dilakukan sekali sehari pada malam hari, sementara kerusakan sistem

atau storage dapat terjadi beberapa menit sebelum proses backup dijalankan, maka nilai RPO adalah 24 jam. Dengan kata lain RPO merupakan pernyataan berapa lama suatu informasi/data boleh hilang.

2.1.3 Teknik Menangani Risiko

Berikut adalah langkah-langkah menangani risiko yaitu:

1. Menghindari Risiko

   Cara ini dilakukan dengan tidak melakukan aktifitas yang dapat mendatangkan risiko. Dalam hal pengerjaan proyek bisa dilakukan melalui cara merubah rencana proyek untuk menghilangkan risiko. Meskipun tidak semua risiko bisa dihindari sepenuhnya, beberapa risiko masih mungkin dihindari. Beberapa risiko yang mungkin terjadi di tahap awal proyek bisa dihindari dengan mengklarifikasi kebutuhan proyek, mengumpulkan informasi, memperbaiki komunikasi atau memperbaiki kemampuan.

2. Reduksi Risiko

   Meliputi langkah-langkah untuk mengurangi peluang terjadinya risiko. Melakukan tindakan awal untuk mengurangi peluang terjadinya risiko pada proyek akan lebih efektif daripada memperbaiki setelah suatu kejadian berisiko terjadi.

3. Menerima Risiko

   Menerima kerugian jika kejadian yang berisiko terjadi. Ini bisa dilakukan jika risiko yang ditimbulkan kecil. Atau tidak ada cara lain lagi untuk menangani. Penerimaan risiko secara aktif bisa diwujudkan dengan menyiapkan rencana contingency atau cadangan jika risiko yang diperkirakan terjadi.

4. Transfer Risiko

   Mengalihkan risiko ke pihak lain. Cara yang umum dalam bisnis adalah membeli asurasi. Dengan asuransi, kita berusaha mengalihkan risiko ke pihak lain. Bisa saja penanganan suatu risiko jatuh ke beberapa kategori. Misalnya mengurangi risiko sekaligus mengalihkan risiko.

2.1.4 Penilaian Risiko Teknologi Informasi

Penilaian risiko (*risk assesment*) merupakan bagian dari manajemen risiko, penilaian risiko adalah proses untuk menilai seberapa sering risiko tersebut terjadi atau seberapa besar dampak yang terjadi dari risiko. Tujuan utama melakukan analisis risiko adalah untuk mengukur dampak dari potensi ancaman, menentukan berapa besar kerugian yang diderita akibat terjadinya risiko dan hilangnya potensi bisnis.

Dalam menggunakan teknologi, manajemen harus menggunakan proses

analisis yang ketat, menyeluruh, hati-hati dan akurat, untuk mengidentifikasi risiko serta memastikan pengendalian risiko yang diterapkan. Untuk itu penilaian risiko yang dilakukan perusahaan perlu dilakukan dengan suatu siklus yang minimal mencakup empat langkah penting sebagai berikut:

1. Pengumpulan data atas aktivitas terkait TI yang berpotensi menimbulkan atau meningkatkan risiko baik dari kegiatan yang akan maupun sedang berjalan termasuk namun tidak terbatas pada:
   (a) Aset TI yang kritikal, dalam rangka mengidentifikasi titik-titik akses dan penyimpangan terhadap informasi yang bersifat rahasia.
   (b) Hasil *review* rencana strategis bisnis, khususnya *review* terhadap penilaian risiko potensial.
   (c) Hasil due dilligence dan pemantauan terhadap kinerja pihak penyedia jasa; Hasil *review* atas laporan atau keluhan yang disampaikan oleh nasabah danatau pengguna TI ke *Call Center* dan atau *Help Desk* Hasil *Self Assessment* yang dilakukan seluruh satuan kerja terhadap pengendalian yang dilakukan terkait TI.
   (d) Temuan-temuan audit terkait penyelenggaraan dan penggunaan TI.
2. Analisis risiko berkaitan dengan dampak potensial dari tiap-tiap risiko, misalnya dari *fraud* di pemrograman, *virus* komputer, kegagalan sistem, bencana alam, kesalahan pemilihan teknologi yang digunakan, masalah pengembangan dan implementasi sistem, kesalahan prediksi perkembangan bisnis Perusahaan.
3. Penetapan prioritas pengendalian dan langkah mitigasi yang didasarkan pada hasil penilaian risiko Perusahaan secara keseluruhan. Untuk itu Perusahaan harus membuat peringkat risiko berdasarkan kemungkinan kejadian dan besarnya dampak yang dapat ditimbulkan serta mitigasi risiko yang dapat dilakukan untuk menurunkan eksposure risiko tersebut.
4. Pemantauan kegiatan pengendalian dan mitigasi yang telah dilakukan atas risiko yang diidentifikasi dalam periode penilaian risiko sebelumnya.

2.1.5 Manajemen Risiko

Manjemen Risiko adalah proses untuk mengidentifikasi risiko, menganalisa risiko, mengukur, memastikan dan melakukan penanganan untuk mengurangi dan mengelola risiko tersebut sampai dampaknya terhadap proses bisnis diorganisasi pada level yang dapat diterima atau diperbolehkan. Risiko ini diukur berdasarkan dampak atau pengaruh yang ditimbulkan terhadap kemungkinan terjadinya risiko.

2.2 Manajemen Risiko Teknologi Informasi

Menurut Stoneburner, Goguen, dan Feringa (2002), Manajemen risiko merupakan proses yang memungkinkan manajer atau penanggung jawab TI untuk menyeimbangkan dan memperhitungkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan risiko dalam upaya melindungi sistem TI dan asset data yang mendukung misi organisasi.

Menurut Nugraha (2016), manajemen risiko merupakan suatu proses atau tindakan yang memungkinkan pemimpin organisasi untuk dapat menyeimbangkan biaya operasional dan ekonomi yang dikeluarkan untuk mengurangi risiko dan mencapai keuntungan dengan melindungi sistem, aset teknologi informasi dan data-data sebagai pendukung misi atau tujuan bisnis.

Menurut Hanafi (2009), manajemen risiko pada dasarnya dilakukan melalui proses identifikasi risiko, evaluasi dan pengukuran risiko serta pengelolaan risiko.

Menurut Hanafi (2009) risiko dapat dikelompokan kedalam enam tipe, yaitu:

1. Risiko murni adalah risiko dimana kemungkinan kerugian ada tetapi tidak untuk kemungkinan keuntungan.
2. Risiko spekulatif adalah risiko dimana pemilik sistem mengharapkan terjadinya kerugian dan juga keuntungan.
3. Risiko status muncul dari kondisi keseimbangan tertentu seperti risiko yang muncul dari kondisi alam yang tidak dapat dihindari.
4. Risiko dinamis muncul dari perubahan kondisi tertentu seperti perubahan teknologi, perubahan kondisi masyarakat dan perubahan lingkungan.
5. Risiko obyektif adalah risiko yang didasarkan pada observasi parameter yang obyektif.
6. Risiko subyektif adalah risiko yang didasarkan pada presepsi seseorang terhadap risiko.

Jadi, manajemen risiko adalah suatu proses identifikasi, mengukur risiko, serta membentuk strartegi untuk mengelolanya melalui sumber daya yang tersedia. Strategi yang dapat digunakan antara lain mentransfer risiko pada pihak lain, menghindari risiko, mengurangi efek buruk dari risiko, dan menerima sebagian maupun seluruh konsekuensi dari risiko tertentu.

Evaluasi kegiatan mempertimbangkan apa yang terjadi selama evaluasi, ketika organisasi yang melakukan evaluasi risiko keamanan informasi, maka untuk melakukan kegiatan dilakukan tahap sebagai berikut:

1. **Identifikasi** yaitu mengidentifikasi risiko keamanan informasi (membuat profil risiko dan informasi organisasi).

2. **Analisis** yaitu menganalisis risiko untuk mengevaluasi risiko dan menetukan prioritas.
3. **Perencanaan** yaitu rencana untuk perbaikan perlindungan oleh pengembangan strategi untuk perbaikan organiasasi dan rencana mitigasi risiko untuk mengurasi risiko terhadap aset penting organisasi. Evaluasi hanya menyediakan arah organisasi sebuah kegiatan keamanan informasi, tidak selalu berarti mengalah keperbaikan. Setelah evaluasi, organisasi harus mengambil langkah-langkah selanjutnya.
4. **Implementasi** yaitu dengan melaksanakan rencana aksi dipilih secara rinci.
5. **Monitor** yaitu dengan memantau kemajuan dan efektifitas, kegiatan ini meliputi pemantauan risiko untuk setiap perubahan.
6. **Kontrol** yaitu Mengontrol pelaksanaanya telah sesuai dengan tindakan korektif, dengan cara menganalisis data, membuat keputusan dan mengeksekusi hasil keputusan yang dibuat.

Hal yang dapat disimpulkan dari mengapa informasi yang dimiliki organisasi harus dilindungi dari ancaman-ancaman yang berpotensi terjadi adalah karena informasi merupakan asset dari organisasi (Nurwibowo, 2014). Manajemen risiko bertujuan memahamkan organisasi perihal:

1. Menentukan seberapa besar dampak atau risiko yang dihadapi oleh organisasi jika terjadi kegagalan keamanan informasi dalam organisasi.
2. Apa saja ancaman (threat) terhadap informasi organisasi dan juga kelemahan (*vulnerability*) yang dimiliki oleh informasi organisasi yang dapat menyebabkan kegagalan keamanan informasi.
3. Bagaimana cara menangani risiko terhadap kegagalan keamanan informasi yang terjadi, dalam hal ini dapat dilakukan atau dipilih cara penanganannya, yaitu dengan cara:
   (a) Menerima dampak atau risiko (*Risk Acceptance*).
   (b) Mengurangi dampak atau risiko (*Risk Reducement*).
   (c) Menghindari atau mengalihkan risiko pada pihak lain (*Risk Transfer*).
   (d) Menentukan control keamanan apa yang tepat yang dibutuhkan oleh organisasi untuk memenuhi kriteria manajemen risiko yang telah dilakukan.

Risiko itu suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya risiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Penggunaan Teknologi Informasi dalam kegiatan operasional perusahaan juga dapat meningkatkan risiko yang dihadapi perusahaan

dengan meningkatnya risiko yang dihadapi, perusahaab perlu menerapkan manajemen risiko secara efektif dalam rangka implementasi ERP diperlukan infrastruktur Teknologi Informasi yang memadai.

Risiko TI itu sendiri dapat didefinisikan sebagai komponen yang berkembang dari total Risiko Operasional. Sebagai bisnis semakin tergantung pada TI untuk mengotomatisasi proses dan menyimpan informasi, Manajemen Risiko TI muncul sebagai praktik terpisah. Organisasi di semua sektor dan industri telah mulai mengkonsolidasikan fungsi untuk mengembangkan yang lebih komprehensif, pendekatan terfokus Risiko TI. Risiko TI meliputi keamanan, ketersediaan, kinerja dan kepatuhan elemen, dengan masing-masing poros penggerak dan kapasitas membahayakannya (Nurwibowo, 2014).

2.3 Keamanan Sistem Informasi

Menurut (Rahardjo, 2005) Keamanan informasi adalah bagaimana sebuah organisasi dapat mencegah penipuan (*cheating*) atau paling tidak mendeteksi adanya penipuan disebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

2.3.1 Aspek Keamanan Sistem Informasi

Menurut (Rahardjo, 2005), ada beberapa aspek keamanan informasi adalah sebagai berikut:

1. *Privacy* atau *Confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya *privat* sedangkan *Confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu.
2. *Integrity* aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya *virus*, *Trojan horse*, atau pemakai lain yang mebgubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi.
3. *Authentication* aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi benar-benar asli, orang yang mengakses atau memberikan informasi adalah benar orang yang dimaksud atau server yang dihubungi adalah benar server yang asli.
4. *Availability* ialah berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang dapat menghambat atau meniadakan akses ke informasi.
5. *Access Control* aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (*pub-*

lic, private, confidential, top secret) dan *user* (*guest, admin, top manager*), mekanisme *authentication* dan juga *privacy*. *Access control* seringkali dilakukan dengan menggunakan kombinasi user id atau *password* atau dengan menggunakan mekanisme lain seperti kartu dan biometrics.

6. *Non-repudiation* aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan transaksi.

2.2.2 Serangan Terhadap Keamanan Sistem

Keamanan berhubungan dengan orang-orang yang mencoba mengakses remote secara ilegal. Sebagian besar masalah keamanan terutama disebabkan oleh orang jahat yang mencoba mengambil keuntungan atau mengganggu seseorang. Informasi yang digunakan oleh bisnis dapat berupa record computer, kertas, model skala, prototipe dan lain.

Security attack, atau serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi (Rahardjo, 2005). Ada beberapa kemungkinan serangan (*attack*) adalah sebagai berikut:

1. *Interruption*
   Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ini biasanya ditujukan kepada tidak ketersediaan (*availability*) dari sistem.
2. *Interception*
   Pihak yang tidak berwenang berhasil mengakses aset atau informasi perusahaan.
3. *Modification*
   Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) asset yang tentu saja dapat merugikan perusahaan.
4. *Fabrication*
   Pihak yang tidak berwenang menyisipkan objek palsu kedalam sistem. Berisi pesan-pesan palsu yang merugikan pemilik sistem.

2.2.3 Tujuan Utama menyediakan Keamanan

Tujuan utama menyediakan keamanan:

1. Kerahasiaan (*confidentiality*) adalah keterjaminan bahwa informai pada sistem komputer hanya dapat diakses oleh pihak-pihak otoritas dan modifikasi dilakukan dengan tetap menjaga keutuhan dan konsistensi data sistem tersebut.
2. Integritas (*integrity*) adalah keterjaminan bahwa sumber sistem hanya dapat di modifikasi oleh pihak-pihak yang otoritas.

3. Ketersediaan (*availability*) adalah keterjaminan bahwa sumber daya sistem komputer telah tersedia bagi pihak-pihak yang diotoritasi saat diperlukan.

2.4 Pengertian Ancaman, Kemungkinan dan Dampak

Berikut adalah pengertian dari Ancaman, Kemungkinan, dan Dampak, yaitu:

2.4.1 Ancaman

Menurut NIST (2012). Ancaman adalah setiap keadaan atau peristiwa yang berpotensi menimbulkan dampak yang dapat merugikan terhadap operasi sistem, aset, individu dan organisasi lain melalui akses yang tidak sah, perusakan, pengungkapan atau modifikasi informasi. Peristiwa ancaman terjadi disebabkan oleh sumber-sumber ancaman yang berpotensial menjadi risiko.

2.4.2 Kemungkinan

Menurut NIST (2012). Kemungkinan kejadian adalah faktor risiko yang bertimbang berdasarkan analisis kemungkinan dari ancaman yang diberikan apakah mampu memanfaatkan kerentanan/kecenderungan yang diberikan (atau serangkaian kerentanan). Faktor risiko kemungkinan menggabungkan perkiraan kemungkinan bahwa peristiwa ancaman akan memperkirakan kemungkinan berdampak yaitu: kemungkinan bahwa hasil kejadian ancaman berdampak merugikan aset informasi.

2.4.3 Dampak

Menurut NIST (2012). adalah benturan, pengaruh atau kejadian yang mendatangkan akibat negatif. Dampak yang terjadi di identifikasi melalui besarnya ancaman atau kemungkinan yang terjadi, yang berhasil mengeksploitasi kerentanan sehingga menyebabkan potensi besarnya dampak.

2.5 Metode Pengukuran Risiko TI

Dalam melakukan proses pengukuran risiko teknologi informasi penulis membutuhkan metode yang dapat dijadikan pedoman. Berikut adalah beberapa metode yang tersedia dalam melakukan pengukuran risiko keamanan teknologi informasi. Diantaranya metode NIST SP 800-30, OCTAVE- S, dan COBIT untuk perbandingan.

NIST (*National Institute of Standard and Technology) Special Publication* (SP) 800-30 merupakan panduan manajemen risiko untuk sistem teknologi informasi yang merupakan standar pemerintah Amerika Serikat (Elky, 2007). Metodologi ini dirancang untuk menjadi suatu perhitungan kualitatif dan didasarkan pada analisa keamanan yang sesuai dengan keinginan pemilik sistem dan ahli teknis un-

tuk benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem TI. Proses ini sangat komprehensif, meliputi segala sesuatu dari ancaman sumber identifikasi untuk evaluasi berkelanjutan dan penilaian.

NIST mengeluarkan rekomendasi melalui publikasi khusus 800-30 tentang *Risk Management Guide for Information Technology System*. Terdapat 9 proses dalam pengelolaan risiko. Stoneburner dkk. (2002) menjelaskan mengenai panduan dalam menggunakan metode NIST (*National Institute of Standard and Technology*) SP (*Special Publication*) 800-30. Berikut adalah penjelasan lebih rinci mengenai sembilan langkah pada metode NIST:

1. **Karakteristik sistem (*System Characterization*)**
   Dalam menilai risiko untuk sistem TI, langkah pertama adalah menentukan ruang lingkup usaha. Pada tahapan ini, batas-batas terhadap sistem harus diidentifikasi terlebih dahulu, bersama dengan sumber daya dan informasi yang merupakan bagian dari sistem tersebut. Karakteristik sistem TI membentuk ruang lingkup dari penialaian risiko, yang menggambarkan batas-batas otorisasi operasional atau akreditasi, dan memberikan informasi (misalnya, perangkat keras, perangkat lunak, interface sistem, data dan informasi, divisi yang bertanggung jawab atau dukungan personil, dan data kritis.
2. **Identifikasi Ancaman (*Threat Identification*)**
   Sumber ancaman didefinisikan sebagai keadaan atau kejadian apa pun yang berpotensi menyebabkan kerusakan pada sistem TI. Sumber ancaman secara umum berasal dari manusia, alami maupun lingkungan. Langkah ini mengidentifikasi ancaman yang akan menyerang kelemahan sistem TI, sebuah kelemahan atau kerentanan dapat dipicu secara tidak sengaja ataupun dieksploitasi dengan sengaja. Sebuah sumber ancaman tidak menghadirkan risiko ketika tidak ada ancaman. Dalam mempertimbangkan kemungkinan adanya ancaman risiko, hal yang tidak boleh diabaikan yaitu mempertimbangan sumber ancaman, potensi kerentanan, dan kontrol yang ada.
3. **Identifikasi Kerentanan (*Vulnerability Identification*)**
   Tujuan dari langkah ini adalah untuk mengembangkan daftar kerentanan sistem teknis dan non-teknis (kekurangan atau kelemahan) yang dapat dimanfaatkan atau dipicu oleh sumber-sumber ancaman-potensial. Kerentanan dapat berkisar dari kebijakan yang tidak lengkap atau bertentangan yang mengatur penggunaan komputer organisasi untuk perlindungan memadai untuk melindungi fasilitas peralatan komputer ke sejumlah perangkat lunak, perangkat keras, atau kekurangan lain yang terdiri dari jaringan komputer organisasi. *Output* - Sebuah daftar kerentanan sistem (pengamatan) yang

dapat dieksekusi oleh sumber ancaman-potensial.

4. **Analisis Kontrol (*Control Analysis*)**

Tujuan dari langkah ini adalah untuk melakukan analisa pengendalian yang telah diimplemantasikan atau direncanakan untuk meminimalkan atau menghilangkan kemungkinan-kemungkinan ancaman dari kelemahan dan kekurangan yang ada.

5. **Penentuan Kemungkinan (*Likelihood Determination*)**

Untuk mendapatkan keseluruhan penilaian terhadap kemungkinan atau kecenderungan yang menunjukan adanya peluang kelemahan yang dapat dilakukan oleh lingkungan ancaman. Berikut ini faktor-faktor yang harus dipertimbangkan seperti motivasi dan sumber ancaman, sifat dari kerentanan, dan keberadaan dan efektifitas pengendalian saat ini dapat dilihat di Tabel 2.1.

Tabel 2.1. Definisi Kemungkinan/Kecenderungan

Tingkat Kemungkinan	Definisi Kemungkinan
Tinggi	Sumber ancaman yang mempunyai motivasi tinggi yang dapat merugikan perusahaan atau instansi, hal ini terjadi karena pengendalian untuk mencegah kerentanan yang dilakukan tidak efektif.
Sedang	Sumber ancaman yang dapat merugikan instansi, tetapi instansi tersebut masih dapat melakukan control di tempat yang dapat menghambat keberhasilan dari kerentanan.
Rendah	Sumber ancaman yang memiliki motivasi rendah, kontrol digunakan untuk mencegah atau secara signifikanm mengurangi atau menghambat suatu kerentanan yang akan terjadi di dalam perusahaan.

6. **Analisis Dampak (*Impact Analysis*)**

Tujuan dari langkah ini adalah untuk menentukan tingkat dampak negatif yang akan dihasilkan dari ancaman berhasil mengeksploitasi kerentanan. Faktor data dan sistem untuk mempertimbangkan harus mencakup pentingnya misi organisasi, kepekaan dan kekritisan (nilai atau kepentingan), biaya yang terkait, hilangnya kerahasiaan, integritas, dan ketersediaan sistem dan data. Besaran Peringkat dampak rendah (10), menengah (50), atau tinggi (100). Rujuk ke SP NIST 800-30 definisi rendah, menengah, dan tinggi Tabel 2.2.

Tabel 2.2. Definisi Besarnya Dampak

Besarnya Dampak	Defenisi Dampak
Tinggi	(a) Dapat mengakibatkan kehilangan yang sangat tinggi dari aset atau sumber daya berwujud utama yang sangat mahal. (b) Dapat secara signifikan melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. (c) Dapat menyebabkan kematian manusia atau cedera serius.
Sedang	(a) Dapat mengakibatkan kehilangan yang sangat tinggi dari aset atau sumber daya berwujud utama yang sangat mahal. (b) Dapat melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. (c) Dapat menyebabkan cedera pada manusia.
Rendah	(a) Dapat mengakibatkan hilangnya beberapa asset atau sumber daya (b) Secara nyata dapat mempengaruhi misi, reputasi, atau minat organisasi.

7. **Penentuan Risiko (*Risk Determination*)**

Tujuan dari langkah ini adalah untuk melakukan penilaian terhadap tingkat risiko bagi sistem TI. Penentuan tingkat risiko ini merupakan suatu fungsi kecenderungan sumber ancaman menyerang *vulnerability* dari sistem TI, Besaran dampak yang akan terjadi jika sumber ancaman sukses menyerang vulnerability dari sistem TI. Terpenuhinya perencanaan kontrol keamanan yang ada untuk mengurangi dan menghilangkan resiko. Rumus penilaian risiko adalah sebagai berikut dan dapat dilihat pada Tabel 2.3:

$$PenilaianRisiko = DampakxPeluang \quad (2.1)$$

Tabel 2.3. Definisi Tingkat Risiko

Skor	Tingkat Risiko	Defenisi Risiko
50-100	**Tinggi**	Jika observasi atau pengamatan di evaluasi sebagai risiko tinggi yang dapat mengakibatkan kerugian yang besar secara *financial* dan kontrol yang digunakan dapat mengurangi risiko tersebut, sehingga sesegera mungkin perlu diberlakukan tindakan korektif.
10-50	**Sedang**	Jika pengamatan risiko sedang dan dapat merugikan sebagian besar asset perusahaan. Tindakan korektif diperlukan dan rencana harus dikembangkan untuk memasukkan tindakan ini dalam periode waktu yang wajar.
1-10	**Rendah**	Jika pengamatan di nilai risiko rendah mengakibatkan sebagian kecil kerugian dan kontrol yang dilakukan dapat mengurangi risiko yang terjadi.

8. **Rekomendasi Control (*Control Recommendations*)**

   Selama proses ini, pengendalian yang dapat mengurangi atau mengeliminasi risiko yang diidentifikasi. Tujuan dari rekomendasi pengendalian adalah mengurangi tingkat risiko bagi sistem TI dan data ketingkat yang dapat diterima oleh organisasi. Faktor-faktor yang harus dipertimbangkan dalam rekomendasi pengendalian dan solusi alternatif untuk meminimalkan atau mengeliminasi risiko diidentifikasi:

   (a) Keefektifan dari pilihan yang direkomendasikan
   (b) Perundang-undangan dan peraturan
   (c) Kebijakan organisasi
   (d) Dampak operasional

9. **Dokumentasi**

   Setelah pengukuran risiko selesai (sumber ancaman, dan kerentanan yang telah diidentifikasi, penilaian risiko, dan rekomendasi pengendalian), hasil-hasil yang ada harus didokumentasikan dalam laporan resmi.

2.4. Profil Perusahaan

PTIPD UIN Suska Riau merupakan salah satu Unit Pelaksana Teknis (UPT) dimana pada awal berdirinya bernama Pusat Komputer (PUSKOM). Didirikannya pusat computer saat itu berawal dari ide yang disusun dengan tujuan untuk menterjemahkan rencana strategis UIN Suska Riau yang terangkum dalam Rencana Induk Pengembangan Teknologi Informasi (RIPTI) untuk diharapkan dapat menjadi pusat kegiatan operasional dibidang teknologi informasi, ikut serta dalam usaha peningkatan kualitas pendidikan, pengajaran dan penelitian maupun pengabdian

kepada masyatakat. PTIPD UIN Suska resmi berdiri didasari oleh surat keputusan nomor: 201/R/2006 yang ditandatangani oleh Rektor UIN Suska Riau pada tanggal 24 juli 2006.

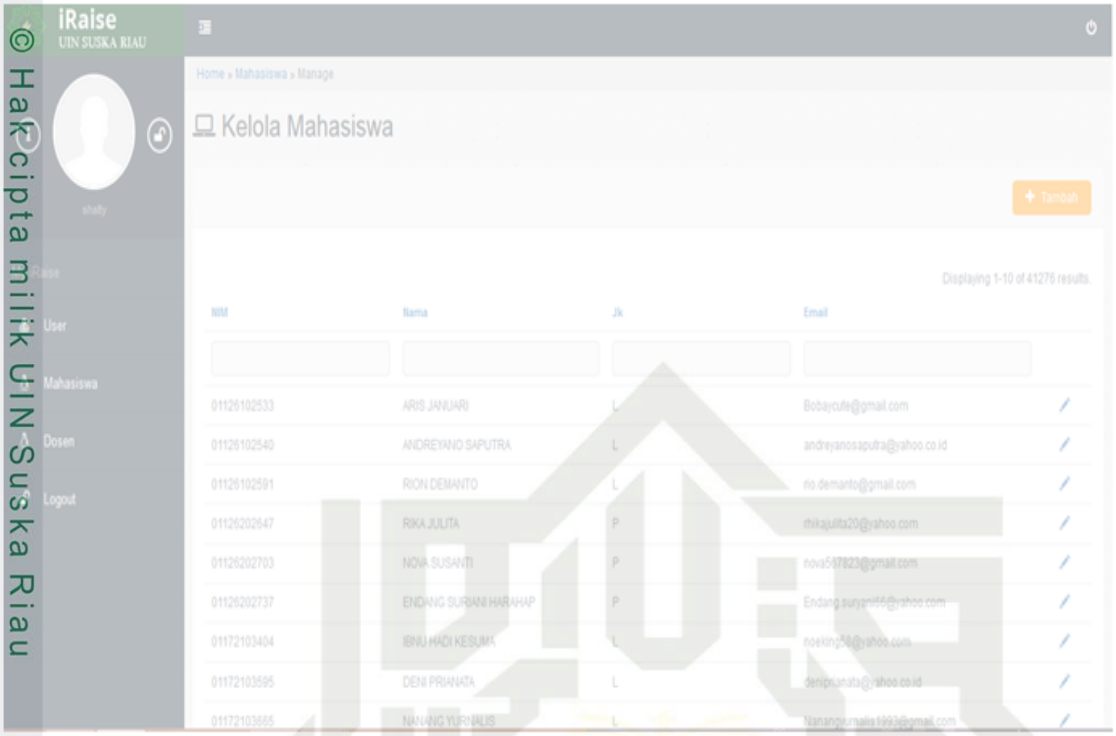
Melalui bantuan IDB UIN Suska Riau pada tahun 2008 PTIPD UIN Suska Riau mendapatkan fasilitas sarana dan prasarana berupa gedung berlantai tiga yang dilengkapi dengan perlatan teknis yang dapat mendukung kegiatan-kegitan operasional pada pusat komputer. Seiring dengan penggunaan internet sebagai jaringan global, UIN Suska Riau pun memperoleh hibah dari pemerintah pusat berupa pembangunan sarana penghubung gedung-gedung utama pada UIN Suska Riau antara lain Gedung Rektorat, Gedung PTIPD, Gedung Perpustakan menggunakan jaringan *fiber optic* (FO). Pada peiode 2008 hingga 2010, PTIPD UIN Suska Riau berhasil membangun infrastruktur jaringan kampus berupa *wireless* dengan kecepatan bandwith 2,5 Mbps yang dapat digunakan civitas akademik UIN Suska Riau untuk aplikasi dan sistem informasi yang digunakan disekitar kampus serta PTIPD juga menyediakan sarana untu keperluan penyimpanan data.

Saat ini mulai dari periode oktober 2014 hingga sekarang PTIPD UIN Suska Riau dipimpin oleh Benny Sukma Negara, M.T, yang diawal masa kepemimpinannya bersama beliau PTIPD UIN Suska Riau telah banyak melakukan perbaikan yang mendasar pada seluruh fasilitas teknologi informasi yang berada di UIN Suska Riau antara lain fasilitas yang menjadi sasaran yaitu optimasi pada fasilitas pendukung jaringan internet, pembenahan pada sistem aplikasi kampus, birokrasi serta pembenahan pada layanan *customer care* yang saat ini semakin mudah dijangkau oleh semua kalangan, dan lain sebagainya. Sehingga pelayanan teknologi informasi di UIN Suska Riau berubah dengan signifikan ke arah yang lebih baik lagi.

Didasari peraturan nomor 9 tahun 2013 yang dikeluarkan oleh Mentri Agama Republik Indonesia tentang organisasi dan tata kerja Universitas Islam Negeri Sultan Syarif Kasim Riau menyatakan, bahwa Pusat Teknologi Informasi dan Pangkalan Data merupakan salah satu Unit Pelaksana Teknis di lingkungan UIN Suska Riau. Dimana PTIPD memiliki tugas untuk mengelola dan ikut seta dalam pengembangan sistem informasi manajemen, pengembangan dan memelihara infrastruktur jaringan dan aplikasi, pengelolaan basis data, pengembangan teknologi informasi dan jaringan kerjasama.

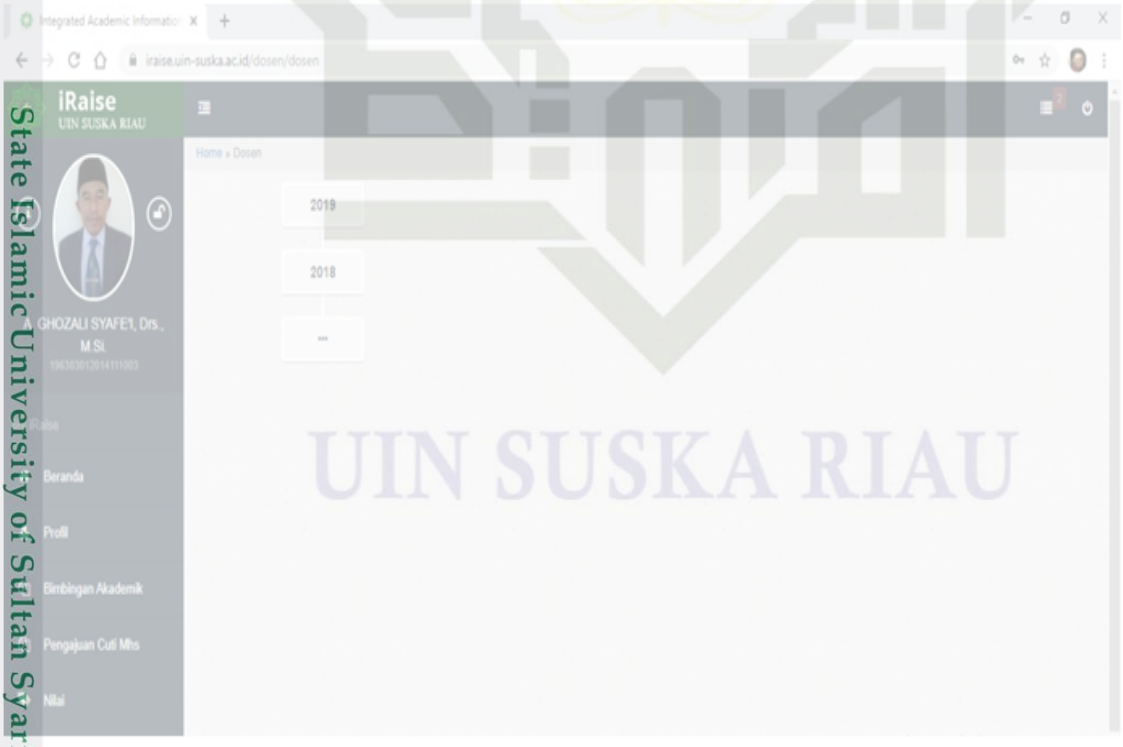
2. Visi, Misi dan Tujuan PTIPD UIN Suska Riau

Mengacu kepada arah perkembangan jangka panjang UIN Suska Riau untuk mendukung hal tersebut maka PTIPD juga memiliki visi, misi tujuan dan sasaran sebagai berikut:



Gambar 4.3. Halaman *Login* Sistem iRaise

Tampilan utama untuk Dosen dapat dilihat pada Gambar 4.4.



Gambar 4.4. Tampilan Halaman Utama Untuk Dosen

4.2 Identifikasi Ancaman (*Threat Identification*)

Tujuan dari langkah ini adalah untuk mengidentifikasi potensi dari sumber ancaman dapat terjadi. Ancaman yang terjadi pada sistem informasi iRaise:

1. Alam: Ancaman yang dapat menimbulkan kerugian secara financial yang sangat besar bagi instansi, yang tidak dapat dihindari.
   Tabel 4.3 menunjukkan gambaran sumber ancaman yang mungkin terjadi disebabkan oleh alam yaitu sebagai berikut:

Tabel 4.3. Identifikasi Sumber Ancaman Alam.

Sumber Ancaman	Sumber Penyebab
Kebakaran	Sambaran petir
Gempa Bumi/Longsor	(a) Lokasi yang tidak strategis (b) Cuaca yang ekstrim
Banjir	(a) Lokasi yang tidak strategis (b) Cuaca yang ekstrim

2. Manusia: Ancaman yang dilakukan secara sengaja atau tidak sengaja.
   Tabel 4.4 menunjukkan gambaran sumber ancaman yang disebabkan oleh manusia yaitu sebagai berikut:

Tabel 4.4. Identifikasi Sumber Ancaman Manusia.

Sumber Ancaman	Tujuan	Penyebab Ancaman
Hacker	(a) Rasa ingin tahu (b) Merubah Data	(a) Kurangnya *security awareness* (b) Tidaknya adanya audit *trail* atau *log*
Virus	Merusak perangkat lunak	(a) Penggunaan *flashdisk* (b) Tidak pernah memperbarui antivirus (c) Mengunduh file sembarangan.

Tabel 4.4 Identifikasi Sumber Ancaman Manusia. (Tabel lanjutan...)

Sumber Ancaman	Tujuan	Penyebab Ancaman
Human Error	Ketidaksengajaan	(a) Perancangan/desain sistem kerja yang kurang baik (b) Manajemen yang tidak menerapkan disiplin secara baik dan ketat (c) Skill dan pengalaman yag kurang memadai
Kebakaran	Merusak perangkat keras dan infrastruktur pendukung	Adanya hubungan pendek arus listrik

3. Teknis: Ancaman yang disebabkan oleh kesalahan teknis
Tabel 4.5 menunjukkan gambaran sumber ancaman yang disebabkan oleh teknis.

Tabel 4.5. Identifikasi Ancaman Teknis.

Sumber Ancaman	Tujuan	Penyebab Ancaman
Kegagalan Jaringan	Tidak disengaja	(a) Jaringan terputus (b) Permasalahan pada provider jaringan.
Kebakaran	Tidak disengaja	Adanya hubungan pendek arus listrik

4.3 Identifikasi Kerentanan (*Vulnerabillity Identification*)

Pada tahapan ini analisa ancaman terhadap sistem harus mencakup analisa kelemahan yang terkait dengan sistem yang dievaluasi. Tujuannya adalah untuk mengembangkan daftar kerentanan atau kelemahan sistem yang dapat dimanfaatkan oleh ancaman sumber potensial. Berikut ini beberapa identifikasi kerentanan yang terjadi di dalam sistem informasi iRaise. Tabel 4.6 merupakan hasil identifikasi yang ada pada sistem berdasarkan hasil wawancara.

Tabel 4.6. Tabel Identifikasi Kerentanan.

Ancaman	Sumber Ancaman	Sumber Kelemahan	Aksi Ancaman
Human Error	Manusia	1. Penyalahgunaan hak akses 2. Sistem ID bekas Karyawan belum di-hapus dari sistem 3. Tamu (magang/Praktek) dapat mengakses sistem secara bebas 4. Karyawan yang ceroboh	1. Merubah data 2. Dapat mengakses data dan informasi iRaise 3. Memanipulasi data-data yang ada pada sistem 4. Terjadi perubahan data se-hingga tidak valid
Virus	Manusia	Pemakaian Flashdisk yang tidak tertib	Merusak data sensitive iRaise

4.4 Analisa Kontrol (*Control Analysis*)

Pada tahan ini bertujuan untuk menganalisis kontrol yang ada dan telah di-laksanakan atau yang sedang direncanakan oleh instansi untuk meminimalkan atau menghilangkan kemungkinan adanya ancaman dan kelemahan pada sistem. Berikut ini adalah Tabel 4.7 kontrol untuk pencegahan insiden, Tabel 4.8 kontrol untuk penanganan insiden secara umum dan Tabel 4.9 daftar kontrol saat ini dan rencana kontrol.

Tabel 4.7. Tabel Identifikasi Kerentanan.

Tahap	Kontrol
Pencegahan	1. Melakukan *update* antivirus 2. Melalukan *Vulnerability assessment* terhadap sistem secara periodik. 3. Melakukan monitoring terhadap sistem secara berkala.

Tabel 4.8. Kontrol Untuk Penanganan Insiden Secara Umum.

Tahap	Kontrol
Pencegahan	1. Mengertahui insiden yang telah terjadi pada sistem. 2. Menganalisa sesuatu yang akan datang berdasarkan indikasi yang ada. 3. Melakukan pengkajian terhadap sistem 4. Mendokumentasikan setiap proses investigasi. 5. Mengklasifikasikan insiden berdasarkan kategori.

Tabel 4.9. Daftar Kontrol Saat Ini Dan Rencana Kontrol.

No	Ancaman	Penyebab Ancaman	Risiko	Kontrol Sekarang	Rencana Kontrol
1	Kebakaran	Adanya hubungan arus pendek listrik (korsleting listrik)	Seluruh data dan informasi terhapus	Pengecekan kelayakan peralatan secara berkala	Membuat *disaster recovery plan*
		Adanya instalasi listrik yang tidak benar	Terbakar atau rusaknya tempat penyimpanan data	Membuat data center	Pemasangan instalasi listrik sesuai prosedur
		Tersambar petir	Merusak perangkat keras dan infrastruktur pendukung	Membuat instalasi penangkal petirr	Membuat data *Center Disaster Recovery Planning* (DRP) yang tahan terhadap bencana alam
	Human Error	Perancangan sistem kerja yang kurang baik	Pelaporan data yang tidak akurat atau tidak tepat	Membuat pembatasan hak akses sesuai tingkat kepentingannya	Melakukan pelatihan dan pengawasan kepada user

Tabel 4.9 Daftar Kontrol Saat Ini Dan Rencana Kontrol. (Tabel lanjutan...)

No	Ancaman	Penyebab Ancaman	Risiko	Kontrol Sekarang	Rencana Kontrol
		Skill dan pengalaman yang kurang memadai Manajemen yang tidak menerapkan SOP	Terjadi kesalahan dalam masalah operasional Pengambilan keputusan yang salah atau kurang tepat	Melakukan pengawalan secara internal berdasarkan jobdesk masing-masing Melakukan perancangan SOP sesuai standar	Melakukan in-house training secara berkala kepada user Menerapkan SOP sesuai stadar yang berlaku
	Virus	Penggunaan Flashdisk yang tidak tertib	Hilangnya data-data penting	Membuat backup data	Mengelompokkan data berdasarkan kegunaannya (Membuat back-up) dan melarang penggunaan *flashdisk* kecuali yang telah disediakan
		Tidak pernah atau jarang memperbarui antivirus	TSoftware tidak dapat diakses	Melakukan update antivirus secara berkala	Memasang antivirus yang berlisensi
		TMengunduh file secara sembarangan atau tidak jelas	Hilang atau rusaknya data-data penting	Melakukan update antivirus secara berkala	Membuat peraturan tertulis mengenai sistem kerja dalam pengunduhan file
	Hacking	Kurangnya *Security awareness*	Merubah dan mengambil data secara illegal	Tidak ada dokumentasi yang dilakukan oleh sistem	Membuat file log sistem dan melakukan backup secara berkala
		Tidak adanya audit *trail* atau *log*	Kehilangan data-data penting yang ada di sistem	Tidak ada dokumentasi yang dilakukan oleh sistem	PBackup data rutin

Tabel 4.9 Daftar Kontrol Saat Ini Dan Rencana Kontrol. (Tabel lanjutan...)

No	Ancaman	Penyebab Ancaman	Risiko	Kontrol Sekarang	Rencana Kontrol
		Enkripsi *password* pengguna masih lemah	*Password* mudah diketahui oleh *hacker*	Enkripsi masih menggunakan MD5	Menggunakan ekripsi yang lebih aman, missal RSA-2048-bit
	Kegagalan Jaringan	ISP (*Internet Service Provider*) terputus	SSistem tidak dapat di akses menggunakan jaringan luar	ISP yang tersedia hanya satu	Penambahan ISP cadangan atau menambah jalur akses cadangan
		Server Down	Sistem tidak dapat di akses, proses pengolahan dan pelaporan terganggu.	Spesifikasi *server* saat ini belum dapat menangani user sekaligusr	*Upgrade* Spesifikasi server

4.5 Penentuan Kemungkinan (*Likehood Determination*)

Tahapan ini dilakukan untuk mendapatkan penilaian secara keseluruhan yang menunjukkan kemungkinan bahwa potensi kelemahan dapat dilaksanakan didalam membangun lingkungan ancaman terkait, kemungkinan jika potensi kelemahan dapat diidentifikasi oleh sumber ancaman yang dapat di kategorikan kedalam level tinggi, sedang atau rendah dapat dilihat pada Tabel 4.10.

Tabel 4.10. Defenisi Kemungkinan.

Skor	Tingkat Kemungkinan	Definisi Kemungkinan
1.0	**Tinggi**	Sumber ancaman yang mempunyai motivasi tinggi yang dapat merugikan perusahaan atau instansi, hal ini terjadi karena pengendalian untuk mencegah kerentanan yang dilakukan tidak efektif.
10.5	**Sedang**	Sumber ancaman yang dapat merugikan instansi, tetapi instansi tersebut masih bisa melakukan control di tempat yang dapat menghambat keberhasilan dan kerentanan.
0.1	**Rendah**	Sumber ancaman yang memiliki motivasi rendah, kontrol digunakan untuk mencegah atau secara signifikanm mengurangi suatu kerentanan yang akan terjadi di dalam perusahaan.

Tabel 4.11 dibawah ini menggambarkan kemungkinan dari ancaman yang akan terjadi di dalam iRaise UIN Suska riau adalah sebagai berikut:

Tabel 4.11. Kemungkinan Dari Ancaman Yang Terjadi.

No	Ancaman	Penyebab Ancaman	Tingkat Kemungkinan
1	Kebakaran	Adanya hubungan arus pendek listrik.	Sedang.
		Adanya instalasi listrik yang tidak benar	Tinggi
		Tersambar Petir	Rendah
2	*Human Error*	Perancangan sistem kerja yang kurang baik.	Tinggi
		Skill dan pengalaman yang kurang memadai	Tinggi
		Manajemen yang tidak menerapkan SOP	Tinggi
3	*Virus*	Penggunaan *Flashdisk* yang tidak tertib.	Rendah
		Jarang memperbarui antivirus	Sedang
		Mengunduh *file* yang tidak jelas atau sembaranganr	Rendah
4	*Hacking*	Kurangnya *Security awareness*.	Tinggi
		Tidak adanya audit trail atau *log*	Tinggi
		Enkripsi password pengguna masih lemah	Tinggi
5	Kegagalan Jaringan	ISP (*Internet Service Provider*) terputus.	Tinggi
		Server down	Tinggi

4.6 Analisa Dampak (*Impact Analysis*)

Langkah penting berikutnya dalam mengukur tingkat risiko adalah menentukan dampak buruk dari akibat ancaman kelemahan tersebut. Untuk melakukan langkah ini maka diperlukan informasi sebagai berikut:

1. **Analisa dampak misi**

   Adapun misi dari sistem iRaise adalah untuk mengatasi dan memberi solusi dalam bebagai macam kesulitan yang selama ini terjadi dalam proses urusan akademik, dan dalam proses tersebut banyak terjadi berbagai macam ancaman yang dapat terjadi dari berbagai macam pihak. Ancaman-ancaman yang terjadi biasa lamgsung mendapat tindakan agar tidak menimbulkan risiko yang lebih parah, kerugian yang besar bagi perusahaan karena hilangnya asset-aset penting, namun ada beberapa hal ancaman yang tidak

bisa dihindari oleh perusahaan namun bisa diminimalisir risikonya yaitu ancaman yang berasal dari alam.

2. **Penilaian Asset Kritis**

Aset informasi kritis adalah aset yang paling penting bagi sebuah instansi dan akan berdampak kerugian jika asset-aset tersebut diketahui oleh pihak-pihak yang tidak berwenang dan tidak bertanggung jawab, asset di modifikasi tanpa otorisasi, atau yang paling berbahaya adalah jika asset tersebut hilang.

3. **Asset Informasi**

Asset informasi digambarkan sebagai informasi atau data yang bernilai atau sesuatu yang tak terhingga nilainya. Seperti informasi data dosen, informasi data mahasiswa, informasi nilai dan informasi riwayat krs.

4. **Kebutuhan Keamanan**

Kebutuhan yang menunjukkan atau meyakinkan bahwa aset informasi user dilindungi oleh sistem dari pihak yang tidak berwenang. Yang pertama adalah menjaga kerahasiaan yaitu meyakinkan bahwa hanya orang-orang pilihan yang memiliki akses pada aset informasi tersebut. Yang kedua, Integritas yaitu meyakinkan bahwa aset informasi tetap pada kondisi yang diharapkan oleh pemilik dan dapat digunakan untuk tujuan yang diharapkan pemilik. Kemudian yang terakhir adalah ketersediaan yaitu meyakinkan bahwa aset informasi tetap dapat diakses hanya untuk pengguna yang memiliki otoritas.

dari penjelasan diatas dapat didefenisi besar level dampak yang dapaat dilihat pada Tabel 4.12

Tabel 4.12. Defenisi Besarnya *Level* Dampak.

Level	Nilai Dampak	Defenisi
100	Tinggi	1. Dapat mengakibatkan hilangnya aset atau sumber daya berwujud utama yang sangat mahal atau sangat penting. 2. Dapat secara signifikan melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. 3. Dapat menyebabkan kematian manusia atau cedera serius.

Tabel 4.12 Defenisi Besarnya *Level* Dampak. (Tabel lanjutan...)

Level	Nilai Dampak	Defenisi
50	Sedang	1. Dapat mengakibatkan hilangnya aset atau sumber daya berwujud yang mahal. 2. Dapat melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. 3. Dapat menyebabkan cedera pada manusia.
10	Tinggi	1. Dapat mengakibatkan hilangnya beberapa aset atau sumber daya berwujud 2. Secara nyata dappat mempengaruhi misi, reputasi, atau minat organisasi.

Tabel 4.13 dibawah ini adalah tabel yang menggambarkan dampak dari ancaman yang akan terjadi pada sistem informasi iRaise.

Tabel 4.13. Dampak Dari Ancaman Yang Terjadi.

Ancaman	Nilai Dampak	Dampak
Kebakaran	Sedang	Seluruh data dan informasi terhapus
	Tinggi	Rusaknya tempat penyimpanan data
	Rendah	Merusak perangkat keras dan infrastruktur pendukung
Human Error	Tinggi	Pelaporan data yang tidak akurat atau tidak tepat
	Tinggi	Terjadi kesalahan dalam menjalankan operasional peusahaan
	Tinggi	Pengambilan keputusan yang salah atau kurang tepat
Virus	Rendah	Hilangnya data/asset penting
	Sedang	Software tidak dapat di akses
	Tinggi	Hilang atau rusaknya data-data penting
Haking	Tinggi	Perubahan data dan informasi yang tidak terotorisasi
	Sedang	Rusaknya tempat penyimpanan data
	Tinggi	*Password* mudah ditebak oleh *hacker*
Kegagalan Jaringan	Rendah	Sistem tidak dapat diakses menggunakan jaringan luar
	Tinggi	Sistem tidak dapat diakses, proses dan pengolahan pelaporan terganggu

4.7 Penentuan Risiko (*Risk Determination*)

Pada tahapan ini bertujuan untuk menilai tingkat risiko terhadap sistem informasi iRaise. Penentuan risiko dari kemungkinan ancaman yang ada, untuk menilai tingkat risiko terhadap sistem informasi iRaise. Adanya dampak yang menyerang suatu sistem didalam instansi harus di minimalisirkan atau harus dicegah segera mungkin agar risiko tersebut tidak menjadi besar dan merugikan instansi dan kemudian dapat melakukan pencegahan agar risiko berikutnya tidak terjadi terus-menerus. Rumus penilaian risiko adalah sebagai berikut:

$$PenilaianRisiko = DampakxPeluang \tag{4.1}$$

Berdasarkan rumus diatas dapat digunakan untuk menentukan tingkat resiko yang dapat dilihat pada Gambar 4.5.

Threat Likelihood	Impact		
			High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Gambar 4.5. Risk Level Matrix

Pada Tabel 4.14 dibawah ini menggambarkan definisi tingkat risiko dari setiap tingkat yang dapat terjadi yaitu sebagai berikut:

Tabel 4.14. Definisi Tingkat Risiko.

Skor	Tingkat Resiko	Definisi Resiko
≥50-100	Tinggi	Mengakibatkan kerugian yang besar secara financial dan control yang digunakan dapat mengurangi risiko tersebut, sehingga sesegera mungkin perlu diberlakukan tindakan korektif.
≥10-50	Sedang	Merugikan sebagian besar asset perusahaan. Tindakan korektif diperlukan dan rencana harus dikembangkan untuk memasukkan tindakan ini dalam periode waktu yang wajar.

Tabel 4.14 Definisi Tingkat Risiko. (Tabel lanjutan...)

Skor	Tingkat Resiko	Definisi Resiko
≥1-10	Renda	Mengakibatkan sebagian kecil kerugian dan control yang dilakukan dapat mengurangi risiko yang terjadi.

Pada Tabel 4.15 dibawah ini adalah tabel menggambarkan besarnya tingkat risiko ancaman yang disebabkan oleh alam adalah sebagai berikut:

Tabel 4.15. Besarnya *Level* Risiko Yang Disebabkan Oleh Alam.

Ancaman	Penyebab Risiko	Dampak	Level		Kategori Risiko
			Peluang	Dampak	
Kebakaran	Adanya hubungan arus pendek listrik	Seluruh data dan informasi terhapus.	Sedang (0.5)	Sedang (50)	Sedang
	Adanya instalasi listrik yang tidak benar	Rusaknya tempat penyimpanan data.	Tinggi (1.0)	Tinggi (100)	Tinggi (100)
	Tersambar petir	Merusak perangkat keras dan infrastruktur pendukung	Rendah (0.1)	Rendah (10)	Rendah

Pada Tabel 4.16 dibawah ini adalah tabel menggambarkan besarnya tingkat risiko ancaman yang disebabkan oleh manusia adalah sebagai berikut:

Tabel 4.16. Besarnya *Level* Risiko Yang Disebabkan Oleh Manusia.

Ancaman	Penyebab Risiko	Dampak	Level		Kategori Risiko
			Peluang	Dampak	
Human error	Perancangan sistem kerja yang kurang baik	Pelaporan data yang tidak akurat atau tidak tepat	Tinggi (1.0)	Tinggi (100)	Tinggi
	Skill dan pengalaman yang kurang memadai	Terjadi kesalahan dalam menjalankan operasional peusahaan	Tinggi (1.0)	Tinggi (100)	Tinggi
	Manajemen yang tidak menerapkan SOP	Pengambilan keputusan yang salah atau kurang tepat	Tinggi (1.0)	Tinggi (100)	Tinggi
Virus	Penggunaan Flashdisk yang tidak tertib	Hilangnya data/asset penting	Rendah (0.1)	Rendah (10)	Rendah
	Jarang memperbarui antivirus	Software tidak dapat di akses	Sedang (0.5)	Tinggi (100)	Sedang

Tabel 4.16 Besarnya *Level* Risiko Yang Disebabkan Oleh Manusia. (Tabel lanjutan...)

Ancaman	Penyebab Risiko	Dampak	Level		Kategori Risiko
			Peluang	Dampak	
	Mengunduh file yang tidak jelas atau sembarangan	Hilang atau rusaknya data-data penting	Sedang (0,5)	Tinggi (100)	Sedang
Hacker	Kurangnya *Security awareness*	Perubahan data dan informasi yang tidak terotorisasi	Tinggi (1.0)	Tinggi	Tinggi
	Tidak adanya audit trail atau log	Kehilangan data-data penting	Tinggi (1.0)	Sedang (50)	Sedang
	Enkripsi password pengguna masih lemah	*Password* mudah ditebak oleh *hacker*	Tinggi (1.0)	Tinggi (100)	Tinggi

Pada Tabel 4.17 dibawah ini adalah tabel menggambarkan besarnya tingkat risiko ancaman yang disebabkan oleh kesalahan teknis dalah sebagai berikut:

Tabel 4.17. Besarnya *Level* Risiko Yang Disebabkan Oleh Kesalahan Teknis.

Ancaman	Penyebab Risiko	Dampak	Level		Kategori Risiko
			Peluang	Dampak	
Kegagalan Jaringan	ISP (*Internet Service Provider*) terputus	Sistem tidak dapat diakses menggunakan jaringan luar.	Tinggi (1.0)	Rendah (10)	Rendah
	Server down	Sistem tidak dapat diakses, proses dan pengolahan pelaporan terganggu.	Tinggi (1.0)	Tinggi (100)	Tinggi

4.3 Rekomendasi Kontrol (*Control Recommendations*)

Tujuan dari rekomendasi kontrol adalah untuk mengurangi tingkat risiko pada sistem informasi iRaise yaitu dengan memberikan rekomendasi terhadap kebijakan yang sudah ada atau yang sudah di lakukan terkait dengan penilaian risko.

1. Menetapkan kebijakan terkait ancaman yang terjadi pada sistem informasi iRaise UIN Suska riau
2. Kebijakan keamanan sistem informasi
3. Keamanan dan kehandalan

Tabel 4.18 berikut ini adalah tabel rekomendasi pengendalian keamanan kontrol yang harus di lakukan oleh PTIPD untuk mengurangi risiko dan mengamankan

data-data yang ada di dalam sistem informasi iRaise dari ancaman yang dapat terjadi yaitu sebagai berikut:

Tabel 4.18. Rekomendasi Kontrol.

Sumber Ancaman	Motivasi	Tindakan Ancaman	Rekomendasi Pengendalian Keamanan
Kebakaran	Tidak disengaja	1. Karena adanya arus pendek aliran listrik 2. Terkena sambaran petir 3. Instalasi listrik yang tidak benar	1. Membuat *distater recovery plan* 2. Membuat *data center distater recovery center* yang kuat dan tahan terhadap bencana alam 3. Melakukan backup dan memasang instalasi listrik sesuai prosedur 4. Mengaktifkan kembali fungsi hydrant
Human Error	Tidak disengaja	1. Menginputkan data tidak benar 2. Penyalahgunaan hak akses 3. Merusak data pada media penyimpanan	1. Melakukan pengawasan kepada pegawai 2. Melakukan in-house training secara berkala kepada user 3. Melakukan pengawasan secara internal terhadap apa saja dikerjakan

Tabel 4.18 Rekomendasi Kontrol. (Tabel lanjutan...)

Sumber Ancaman	Motivasi	Tindakan Ancaman	Rekomendasi Pengendalian Keamanan
Virus	Pengerusakan	1. Kegagalan operasi software 2. Perubahan data 3. Rusak atau kehilangan data	1. Menggunakan antivirus yang berlisensi 2. Mengelompokan data berdasarkan kegunaannya secara jelas lalu membuat backupnya 3. Membuat peraturan tertulis tentang sistem pengunduhan file
Hacker	Pengerusakan	1. Penyelundupan File (Penyelundupan File) 2. Perubahan data dan informasi 3. Pencurian data	*Update* kode sistem dan memperbaiki celah yang rentan agar sistem lebih handal.
Kegagalan Jaringan	Tidak disengaja	Permasalahan pada provider jaringan	Meningkatkan kehandalan jaringan dengan melakukan redudansi perangkat jaringan pendukung sistem iRaise sebagai backup jika salah satunya mengalami gangguan.

4.9 Dokumentasi

Setelah penilaian risiko selesai hasilnya harus di dokumentasikan ke dalam bentuk laporan. Dokumentasi menggambarkan keseluruhan proses penilaian risiko, mulai dari ancaman dan kerentanan, pengukuran risiko dan rekomendasi *control*

untuk diimplementasikan. Dari hasil laporan dapat membantu manajemen instansi untuk membuat sebuah keputusan tentang perubahan kebijakan, prosedur, maupun anggaran. Dokumentasi terdapat pada bagian Lampiran A, Lampiran B, Lampiran C dan Lampiran D.

BAB 5
PENUTUP

5.1 Kesimpulan

Penelitian telah dilakukan pada PTIPD UIN Suska Riau, dimana penelitian dilakukan dengan cara mengukur risiko sistem informasi akademik yaitu iRaise dengan menggunakan metode NIST SP 800-30. Berdasarkan penelitian yang telah dilakukan dapat disimpulkan beberapa hal sebagai berikut:

1. Pada proses pengolahan data dihasilkan ancaman-ancaman yang sudah teridentifikasi. Ancaman yang terjadi pada sistem informasi iRaise yaitu kebakaran, human error, virus, hacking dan kegagalan jaringan. Ancaman ancaman tersebut yang kerap kali timbul dan menjadi permasalahan selama pelayanan akademik berjalan dan menyebabkan proses layanan terganggu.
2. Pada proses identifikasi ancaman yang terjadi pada sistem informasi iRaise telah ditemukan tingkat risiko yang berbeda pada tiap kategori. Level risiko yang diidentifikasi berdasarkan dari hasil perhitungan kuesioner.
3. Hasil dari penilaian risiko yang terjadi pada sistem informasi iRaise memberikan rekomendasi kontrol yang disarankan terhadap ancaman risiko yang terjadi, sehingga dapat menjadi acuan bagi instansi untuk dapat digunakan untuk kontrol selanjutnya.

5.2 Saran

Beberapa saran yang dapat dijadikan masukan antara lain:

1. Melakukan pembaharuan informasi terhadap sistem dengan mengumpulkan risiko-risiko secara rutin yaitu sekali dalam setahun sehingga dapat meminimalkan terjadinya risiko atau mencegah risiko yang akan terjadi.
2. Membuat pendokumentasian untuk setiap prosedur dan kejadian risiko yang ada, sehingga memudahkan aktivitas audit dan memperkecil risiko internal yang terjadi di PTIPD.
3. Manajemen risiko dapat berjalan dengan baik jika adanya dukungan dengan komitmen manajemen level atas dan partisipasi bagian rektorat, serta kesadaran dan kerjasama dari seluruh penanggung jawab yang harus mengikuti prosedur dan mematuhi kontrol yang telah ditetapkan.

DAFTAR PUSTAKA

Eky, S. (2007). An introduction to information systems risk management.

Febriyanti, A., dan Hidayanto, B. C. (2012). Manajemen risiko pada pengelolaan data di bagian pengolahan data pt petrokimia gresik. *Jurnal Teknik Pomits*, *1*(1), 1–6.

Gondodiyoto, S. (2007). Audit sistem informasi. edisi revisi. *Jakarta: Mitra Wacana Media*.

Hanafi, M. M. (2009). Manajemen risiko edisi kedua. *Yogyakarta: UPP STIM YKPN*.

Hubbard, D. (2009). *The future of risk management: Why it's broken and how to fix it.* John Wiley & Sons.

NIST. (2012). Nist sp 800-30 revision 1: Guide for conducting risk assessments. , *1*(02), 1-95.

Nugraha, U. (2016). Manajemen risiko sistem informasi pada perguruan tinggi menggunakan kerangka kerja nist sp 800-300..

Nurwibowo, P. (2014). *Penilaian risiko penggunaan teknologi informasi menggunakan metode octave-s (studi kasus: Pt qnb kesawan)* (Unpublished doctoral dissertation). Universitas Islam Negeri Sultan Syarif Kasim Riau.

Rahardjo, B. (2005). Keamanan sistem informasi berbasis internet. *Bandung: PT. Insan Indonesia*.

Stoneburner, G., Goguen, A., dan Feringa, A. (2002). Risk management guide for information technology systems. *Nist special publication*, *800*(30), 800–30.

Syalim, A., Hori, Y., dan Sakurai, K. (2009). Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft's security management guide. Dalam *2009 international conference on availability, reliability and security* (hal. 726–731).

Tarsito, S. (2014). Metode penelitian kuantitatif, kualitatif dan r&d. *Alfabeta. Bandung*.

Wiyanto, A. R., Latuihamallo, O. S., Tua, F. M., Gui, A., dan Suryanto, S. (2013). Manajemen risiko teknologi informasi: Studi kasus pada perusahaan jasa. *ComTech: Computer, Mathematics and Engineering Applications*, *4*(1), 43–54.

LAMPIRAN A
DAFTAR WAWANCARA

1. **P : Apa saja ruang lingkup kerja PTIPD?**
   J : PTIPD adalah organisasi unit pelaksana teknis di UIN SUSKA Riau yang bertugas mengelola dan melayani aktifitas yang berkaitan dengan teknologi informasi dan layanan data berikut dari segi bisnis yang sangat berpengaruh terhadap perkembangan Universitas.
2. **P : Apakah PTIPD memiliki SOP dan Job Description untuk petugas atau pegawai?**
   J : PTIPD memiliki SOP dan JobDesc berdasarkan divisi yang ada yaitu : divisi adminisitrasi, keuangan, infrastruktur jaringan, sumberdaya informasi aplikasi, sistem jaringan dan pangkalan data, komunikasi internet, dan pelatihan atau sertifikasi.
3. **P : Apa saja sistem informasi yang dikelola PTIPD beserta rencana kedepannya?**
   J : Sistem informasi akademik IRaise, Kepegawaian, SIREG, Repository, KKN, RPG (Realtime Payment Gateway), Wisuda, PMB, aplikasi pengendali keuangan IGrasy dan Verdana (Verifikasi dan pencairan dana), aplikasi pendidikan dan pengajar terpadu, VoIp, i-Smail, Manajemen layanan IT dan lainnya.
4. **P : Apa saja permasalahan teknis dan non teknis yang terjadi di P-TIPD?**
   J : Permasalahan teknis yaitu dibutuhkan tambahan personel untuk meningkatkan efektifitas dan pengembangan pada tiap divisi, termasuk pembagian tiap-tiap fakultas yang ada. Permasalahan non teknis Sebagian besar pegawai masih membutuhkan pemahaman masalah yang berkaitan dengan teknologi informasi seperti masalah sederhana mengenai billing internet.
5. **P : Sejak kapan iraise diimplementasikan?**
   J : Februari 2015 (Pada awal semester)
6. **P : Pihak yang membuat iraise ?**
   J : Pihak PTIPD dan developer, pihak developernya terdiri dari beberapa perusahaan.
7. **P : Bahasa pemrograman apa yang di gunakan, besaran bandwidth dan database server ?**
   J : Bahasa pemrograman YII, bandwidthnya 500 MB, MySQL
8. **P : Apakah pernah dilakukan sosialiasai irase ?**
   J : Pernah, bahkan sering. Karena biasanya kita tiap semester mengadakan sosialisasi dengan mahasiswa baru dan dosen.

9. **P : Apakah ada pembatasan hak akses pada iraise ?**

   J : Tentu ada, untuk mahasiswa beda dosen juga begitu. Ada hak nya masing-masing dan di bedakan melalui username dan passwordnya

10. **P : Apa saja permasalahan keamanan informasi atau risiko yang pernah terjadi?**

    J : Permasalahan internal yaitu belum rapinya dokumentasi aktifitas teknis, konfigurasi dan topologi jaringan yang mungkin belum maksimal pada sebagian fakultas termasuk permasalahan listrik dan hal yang berkaitan dan menyebabkan permasalahan jaringan internet, masalah backup data, keluhan jaringan internet lambat, human error. Permasalahan eksternal yaitu serangan yang dilakukan anonym seperti web deface, dan segala bentuk serangan dari sisi jaringan, hingga percobaan akses data penting. Risiko atau ancaman tentunya ada karena hal ini terus berkembang atau selalu ada cara baru terhadap penyadapan informasi, risiko dari lingkungan server seperti sniffing password melalui jaringan yang sama, dari sisi human error yang dapat berpengaruh pada social engineering dan teknik penyerangan lainnya.

11. **P : Apa penyebab risiko itu terjadi?**

    J : Seperti permasalahan teknis kekurangan personil, SOP yang belum lengkap, infrastruktur yang belum lengkap karena membutuhkan belanja modal yang besar, aplikasi yang dibuat mengejar waktu sehingga belum adanya audit diawal.

12. **P : Bagaimana cara PTIPD dalam mengatasi masalah keamanan informasi?**

    J : Dari segi infrastruktur yaitu dengan adanya firewall, memisahkan database aplikasi – aplikasi akademik dengan yang lainnya, mengatur SOP dengan menyisipkan aspek keamanan dan manajemen risiko seperti akses, backup data, recovery data, dan pada teknisi dilakukan pelatihan-pelatihan

SURAT KETERANGAN
TELAH MELAKUKAN WAWANCARA

Yang bertanda tangan di bawah ini:
Nama : Dziki Adli, S.T
Jabatan : Kepala Divisi Sistem Jaringan dan Pangkalan Data

Menerangkan bahwa mahasiswa yang teridentitas di bawah ini :
Nama : Yusrika Dewi
Jurusan : Sistem Informasi
Semester : X (Sepuluh)
Fakultas : Sains dan Teknologi UIN Suska Riau

Benar telah melakukan wawancara untuk penelitian Tugas Akhir dengan judul "Manajemen Risiko IT pada Siste Iraise Menggunakan Metode NIST SP 800-30 (Studi Kasus: PTIPD UIN Suska Riau)". Demikian surat keterangan ini untuk dapat dipergunakan sebagaimana mestinya.

Narasumber

Dziki Adli, S.T

1. **P : Apa saja infrastruktur yang mendukung Iraise?**
   J : Yang pertama jaringan, lalu data center beserta seluruh komponennya seperti server dan lain-lain, keamanan sistem dan aplikasi itu sendiri beserta pengelolanya
2. **P : Apa saja data yang bersifat sensitif pada Iraise?**
   J : Sebenarnya semua yang ada di iraise bersifat sensitive karena saling berkaitan. Terdapat data dosen, mata kuliah beserta kelas dan yang paling utama tentunya adalah nilai mahasiswa .
3. **P : Apakah pernah dilakukan penilaian risiko pada Iraise?**
   J : Penilaian risiko belum pernah, pernah mencoba membuat manajemen risiko namun belum tuntas dan audit hanya pada tata kelola data center.
4. **P : Seberapa sering iRaise dilakukan maintenance?**
   J : Ada yang rutin, ada yang by incident. Kalau yang rutin kita selalu melakukan pemeliharaan boleh dibilang harian. Kalau yang by incident misalnya terjadi permasalahan-permasalahan yang di luar standar dalam penginputan data seperti mata kuliah, kelas dan nilai dan lain-lain
5. **P : Kenapa iraise sering down saat pengisian KRS berlangsung?**
   J : Kalau pada masalah down itu karena spesifikasi pada servernya belum memadai, hardware nya belum sanggup jika menampung traffic yang terlalu tinggi jadi makanya kenapa pengisian krs itu dipecah-pecah atau di buat jadwal.
6. **P : Kapan terakhir kali di update ?**
   J : Update gak bisa karena sistem ini berbentuk fortal, paling hanya penambahan fitur dari programmer jadi langsung terbarui otomatis
7. **P : Adakah tenaga ahli yang menangani masalah keamanan informasi?**
   J : Ada, yaitu saya bagian divisi sistem jaringan data center yang secara teknis mengatasi masalah keamanan informasi.
8. **P : Apa saja masalah keamaman informasi yang pernah dialami beserta ancaman atau risiko keamanan informasi pada Iraise?** J : Kita pernah mengalami serangan seperti web deface, sistem disisipi shell atau backdoor, hal-hal kecil yang juga berpengaruh seperti pengisian krs sebelum melunasi spp, penghapusan mata kuliah yang sudah diambil, pemalsuan aplikasi dalam bentuk mobile, Kabel Fiber Optic yang beberapa kali sempat putus saat kegiatan pembangunan, perangkat disambar petir, dan pemadaman listrik yang menyebabkan jaringan internet terputus dan Iraise tidak dapat di akses yang berdampak terhadap penjadwalan seperti pengisian KRS (Kartu Rencana Studi) yang tidak sesuai dengan waktu yang ditetapkan. Ad-

min bagian akademik masih menggunakan jaringan wireless, sehingga memungkinkan adanya serangan sniffing password. Admin akademik diberi kebebasan menukar password sesuai kehendak dan keperluan tanpa konfirmasi email, hal ini memungkinkan adanya social engineering atau serangan bruteforce.

9. **P : Apa tindakan yang dilakukan dalam mengatasi masalah tersebut?**
J : Yang paling berpengaruh yaitu dengan adanya firewall, yang akan memblokir situs berbahaya, mencatat dan blokir IP aktifitas mencurigakan. Sistem yang dilengkapi human identification. Pemisahan database dan backup data, memperbaiki coding dari bug-bug dalam pemalsuan data dan lainnya, hingga memodifikasi perangkat data center beserta jaringan yang mendukung.

10. **P : Adakah dampak atau kerugian dari masalah keamanan informasi yang sudah terjadi?**
J : Permasalah data atau informasi itu kan sifat nya intangible, tidak ternilai, jadi jika data itu mengalami faktor pelanggaran sistem informasi seperti ketersediaan, intergritas, autentikasi dan sebagainya maka sudah mengalami hal-hal yang merugikan, jika dibilang kerugian tentunya tidak ternilai harganya. Dari segi waktu juga tentunya akan sangat berdampak, akan terjadi keterlambatan 11. P : Apakah dilakukan dokumentasi pada masalah keamanan informasi yang telah terjadi? J : Tidak ada, karena seperti perusahaan kebanyakan bahwa masalah keamanan informasi diketahui setelah kejadian, setelah kita tahu dan mengalami secara langsung, karena pencatatan akan dibuat setelah dilakukan audit secara menyeluruh.

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
FAKULTAS SAINS DAN TEKNOLOGI
كلية العلوم و التكنولوجيا
FACULTY OF SCIENCES AND TECHNOLOGY

Jl. H.R. Soebrantas KM. 18 No. 155 Simpang Baru Panam Pekanbaru 28129 PO. Box. 1004 Telp. 0761-589026-27
Fax 0761-859025, Web Site: www.uin-suska.ac.id, E-mail: fatte@uin-suska.ac.id

Nomor : Un.04/F.V/PP.00.9/6993/2017
Sifat : Penting
Lampiran : -
Hal : Mohon Izin Pengambilan Data Penelitian Tugas Akhir/Skripsi

Pekanbaru, 26 September 2017

Kepada Yth:
Kepala PTIPD UIN Suska Riau
di
Tempat

Assalamu 'alaikum Wr. Wb.,

Dengan hormat, sehubungan mahasiswa kami tersebut di bawah ini:

Nama : Yusrika Dewi
NIM : 11353204459
Fakultas : Fakultas Sains dan Teknologi
Jurusan : Sistem Informasi
Semester : IX (Sembilan)

akan melaksanakan penelitian di Instansi yang Saudara pimpin, guna mendapatkan data dan informasi dalam rangka penyelesaian tugas akhir dengan judul **"Analisis Manajemen Resiko IT pada Penerapan Sistem Iraise Menggunakan Metode Octave-s (Studi Kasus: PTIPD UIN Suska Riau)"**.

Untuk itu, kami mohon kiranya Saudara dapat memberikan izin kepada mahasiswa tersebut melakukan penelitian untuk mendapatkan data yang diperlukan.

Demikian yang dapat kami sampaikan, atas bantuan dan kerjasamanya, kami ucapkan terima kasih.

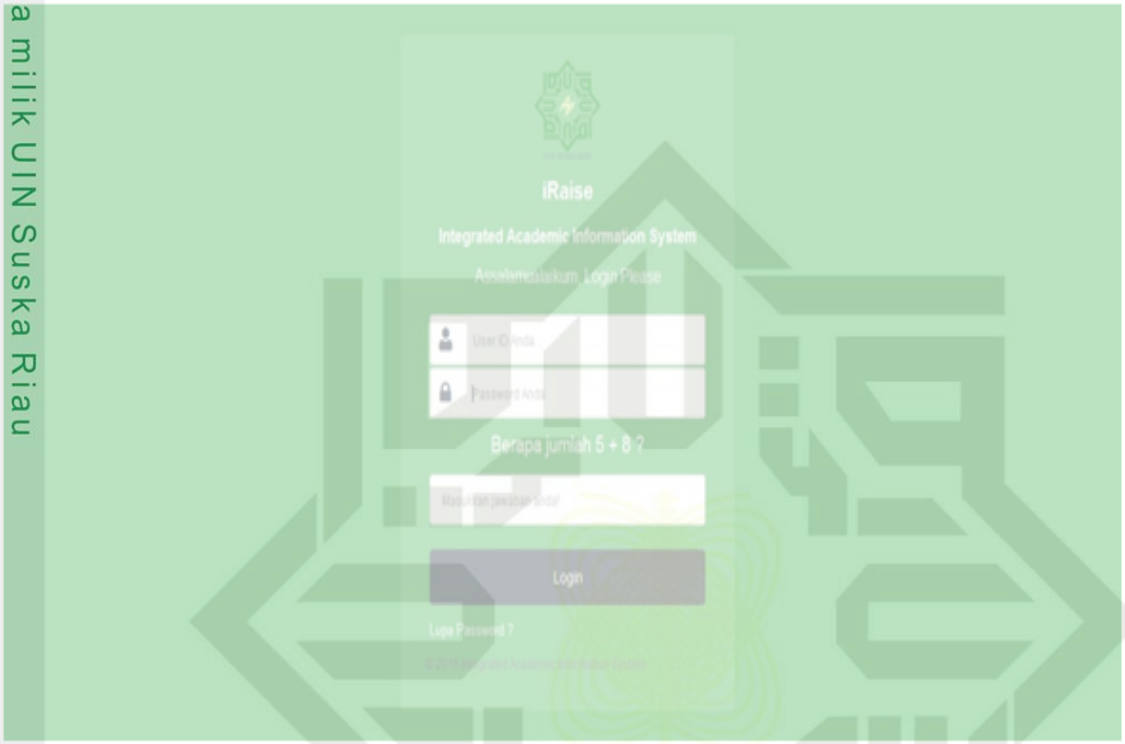
Wassalam
a.n. REKTOR
Dekan,

Dr. Hartono, M.Pd
NIP. 19640301 199203 1 003

Tembusan:
Rektor UIN Suska Riau (sebagai laporan)

LAMPIRAN B
INTERFACE SISTEM

Berikut adalah tampilan halaman login pada sistem iraise:



Tampilam halaman utama atau beranda untuk mahasiswa

Tampilan halaman utama untuk mahasiswa

Tampilan halaman utama untuk admin pengelola

Tampilan utama untuk Dosen

LAMPIRAN C
PENILAIAN KEMUNGKINAN RISIKO

Nama : Benny Sukma Negara, MT.
Jabatan : Kepala PTIPD

Kepada Bapak/Ibu yang saya hormati, saya bermaksud untuk menyerahkan lampiran kuesioner penilaian kemungkinan risiko berbentuk tabel yang berisi daftar pernyataan untuk diisi penilaian terhadap tingkat kemungkinan risiko, kemudian hasil kuesioner ini akan digunakan untuk melakukan perhitungan penilaian risiko pada sistem informasi iraise UIN Suska Riau.

Adapun kriteria penilaian kemungkinan risiko yang tertera pada tabel dibawah ini sebagai berikut:

Tabel 1 : Tingkat Kemungkinan/kecenderungan

Skor	Tingkat Kemungkinan	Definisi Kemungkinan
1.0	Tinggi	Sumber ancaman yang mempunyai motivasi tinggi yang dapat merugikan perusahaan atau instansi, hal ini terjadi karena pengendalian untuk mencegah kerentanan yang dilakukan tidak efektif.
0.5	Sedang	Sumber ancaman yang dapat merugikan instansi, tetapi instansi tersebut masih bisa melakukan control yang mungkin dapat menghambat keberhasilan dan kerentanan.
0.1	Rendah	Sumber ancaman yang memiliki motivasi rendah, control digunakan untuk mencegah atau secara signifikan untuk mengurangi suatu kerentanan yang akan terjadi di dalam perusahaan.

Tabel 2 : Daftar Pertanyaan

No.	Pertanyaan	Skor	Tingkat Kemungkinan
1.	Pada level berapa kemungkinan terjadinya risiko kebakaran, yang disebabkan oleh hubungan arus pendek listrik.	0.5	Sedang
2.	Pada level berapa kemungkinan terjadinya risiko kebakaran, yang penyebabnya karena instalasi listrik yang tidak benar.	1.0	Tinggi
3.	Pada level berapa kemungkinan terjadinya risiko kebakaran, yang disebabkan oleh sambaran petir	0.1	Rendah
4.	Pada level berapa kemungkinan terjadinya risiko *human error,* yang disebabkan oleh perancangan sistem kerja yang kurang baik	1.0	Tinggi
5.	Pada level berapa kemungkinan terjadinya risiko *human error,* yang disebabkan oleh skill dan pengalaman yang kurang memadai	1.0	Tinggi
6.	Pada level berapa kemungkinan terjadinya risiko *human error,* yang disebabkan oleh manajemen yang tidak menerapkan SOP.	1.0	Tinggi
7.	Pada level berapa kemungkinan terjadinya risiko *virus,* yang disebabkan oleh penggunaan *Falshdisk* yang tidak tertib.	0.1	Rendah
8.	Pada level berapa kemungkinan terjadinya risiko *virus,* yang disebabkan oleh jarang memperbarui antivirus.	0.5	Sedang
9.	Pada level berapa kemungkinan terjadinya risiko *virus,* yang disebabkan oleh pengunduhan file yang tidak jelas.	0.5	Sedang

10.	Pada level berapa kemungkinan terjadinya risiko *hacking*, karena kurangnya *Security awareness*	1.0	Tinggi
11.	Pada level berapa kemungkinan terjadinya risiko *hacking,* yang disebabkan oleh tidak adanya *audit trail* atau log	1.0	Tinggi
12.	Pada level berapa kemungkinan terjadinya risiko *hacking,* yang disebabkan oleh enkripsi password pengguna masih lemah	1.0	Tinggi
13.	Pada level berapa kemungkinan terjadinya risiko kegagalan jaringan, yang penyebabnya karena ISP (*Internet Service Provider)* terputus.	1.0	Tinggi
14.	Pada level berapa kemungkinan terjadinya risiko kegagalan jaringan, yang penyebabnya karena server down.	1.0	Tinggi

Narasumber

Benny Sukma Negara
2021.01.24 06:51:19 +07'00'

Benny Sukma Negara, MT.

LAMPIRAN D
PENILAIAN DAMPAK RISIKO

Nama : Benny Sukma Negara, MT.
Jabatan : Kepala PTIPD

Kepada Bapak/Ibu yang saya hormati, saya bermaksud untuk menyerahkan lampiran kuesioner penilaian dampak risiko berbentuk tabel yang berisi daftar pernyataan untuk diisi penilaian terhadap tingkat dampak risiko, kemudian hasil kuesioner ini dapat digunakan untuk melakukan perhitungan penilaian risiko pada sistem informasi iraise UIN Suska Riau.

Tabel 1 : Tingkat Dampak

Level	Nilai Dampak	Defenisi
100	Tinggi	1. Dapat mengakibatkan hilangnya aset atau sumber daya berwujud utama yang sangat mahal. 2. Dapat secara signifikan melanggar, membahayakan, atau menghalangi misi, reputasi, atau kepentingan organisasi. 3. Dapat menyebabkan kematian manusia atau cedera serius.
50	Sedang	1. Dapat mengakibatkan hilangnya aset atau sumber daya berwujud yang mahal. 2. Dapat melanggar, membahayakan, atau menghalagi misi, reputasi, atau kepentingan organisasi. 3. Dapat menyebabkan cedera pada manusia.
10	Rendah	1. Dapat mengakibatkan hilangnya beberapa aset atau sumber daya berwujud 2. Secara nyata dappat mempengaruhi misi, reputasi, atau minat organisasi.

Tabel 2 : Daftar pertanyaan

No.	Pertanyaan	Level Dampak	Kategori Risiko
1.	Pada level berapa dampak terjadinya risiko kebakaran, yang mengakibatkan seluruh data dan informasi terhapus.	50	Sedang
2.	Pada level berapa dampak terjadinya risiko kebakaran, yang mengakibatkan rusaknya tempat penyimpanan data.	100	Tinggi
3.	Pada level berapa dampak terjadinya risiko kebakaran, yang mengakibatkan *hardware* dan infrastruktur pendukung mengalami kerusakan.	10	Rendah
4.	Pada level berapa dampak terjadinya risiko *human error,* yang mengakibatkan pelaporan data menjadi tidak akurat atau tidak tepat.	100	Tinggi
5.	Pada level berapa dampak terjadinya risiko *human error,* yang dapat mengakibatkan pengambilan keputusan yang salah atau kurang tepat	100	Tinggi
6.	Pada level berapa dampak terjadinya risiko *human error,* yang mengakibatkan terjadi kesalahan dalam masalah operasional.	100	Tinggi
7.	Pada level berapa dampak terjadinya risiko *virus,* yang dapat mengakibatkan rusaknya data-data penting perusahaan	10	Rendah
8.	Pada level berapa dampak terjadinya risiko *virus,* yang dapat mengakibatkan hilangnya data-data penting	100	Tinggi

9.	Pada level berapa dampak terjadinya risiko *virus,* yang dapat mengakibatkan *Software* tidak dapat di akses	50	Sedang
10	Pada level berapa dampak terjadinya risiko *hacking,* yang dapat mengakibatkan *Password* mudah ditebak oleh *hacker*	100	Tinggi
11.	Pada level berapa dampak terjadinya risiko *hacking,* yang dapat mengakibatkan data dimanipulasi atau berubahnya data yang tidak terotorisasi	100	Tinggi
12.	Pada level berapa dampak terjadinya risiko *hacking,* yang dapat mengakibatkan instansi mengalami kerugian.	50	Sedang
13.	Pada level berapa dampak terjadinya kegagalan jaringan, yang dapat mengakibatkan segala proses menjadi terhambat karena sistem tidak dapat diakses	50	Rendah
14.	Pada level berapa dampak terjadinya kegagalan jaringan, yang dapat mengakibatkan segala proses penginputan, pengolahan dan pelaporan data terganggu.	100	Tinggi

Narasumber

Benny Sukma Negara
2021.01.24 06:51:19 +07'00'

Benny Sukma Negara, MT.

DAFTAR RIWAYAT HIDUP

Yusrika Dewi, lahir di Medan, Provinsi Sumatera Utara, pada 17 Juni 1995 sebagai anak ke 3 (tiga) dari Bapak Yustiono dan Ibu Rusmini, yang beralamat di Kelurahan Tasik Tebing Serai, Kecamatan Talang Muandau, Kabupaten Bengkalis, Provinsi Riau. Email: yusrika.dewi@students.uin-suska.ac.id, HP: 087872710952. Pengalaman pendidikan yang dilalui mulai SD pada tahun 2001-2007, Selanjutnya pada tahun 2007 melanjutkan pendidikan di Madrasah Tsanawiyah di Pesantren Hubbuwathan Duri, Kab. Bengkalis hingga tahun 2010. Setelah tamat MTs pendidikan dilanjutkan di SMK Negeri 1 Kandis, Kec. Kandis Kab. Siak hingga tahun 2013. Kemudian kuliah di Jurusan Sistem Informasi Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau hingga menyelesaikan Laporan Tugas Akhir ini.

Penelitian tugas akhir berjudul "Manajemen Risiko Sistem Iraise Menggunakan Metode NIST SP 800-30 Pada PTIPD UIN Suska Riau". Selama menjadi mahasiswa, penulis sering mengikuti aktivitas mahasiswa lainnya. Penulis juga pernah melaksanakan Kerja Praktek di PT. Telkomsel, kemudian mengikuti Kuliah Kerja Nyata (KKN) di Desa Balai Pungut, Kecamatan Pinggir, Kabupaten Bengkalis, Provinsi Riau.